NPS-SE-06-003

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

Implication of FORCEnet on Coalition Forces

by

Eric Romero
Jeffrey Gorsch
Arkapol Nantasenamat
Mario Sanchez
Michelle Nguyen
Tewodros Metaferia
Joel Timm
Clara Barron
Vincent Jung
Michael Nguyen
David Tan

September 2006

Approved for public release; distribution is unlimited

Prepared for: Deputy Chief of Naval Operations for Warfare Requirements and Program (OPNAV N71), 2000 Pentagon, TTCP MAR Group, Action Group 6, Washington, DC 20350-2000

THIS PAGE INTENTIONALLY LEFT BLANK

NAVAL POSTGRADUATE SCHOOL
MONTEREY, CALIFORNIA 93943-5001

COL. David A. Smarsh, USAF
Acting President

Leonard A Ferrari
Provost

This report was prepared for the Deputy Chief of Naval Operations for Warfare Requirements and Program (OPNAV N71), 2000 Navy Pentagon, TTCP MAR Group, Action Group 6 Washington, DC 20350-2000.

This report was prepared by the Masters of Science in Systems Engineering (MSSE) Cohort Four from the Port Hueneme Division (PHD) of the Naval Surface Warfare Center (NSWC):

Authors:

Eric Romero	Joel Timm	Clara Barron
Mario Sanchez	Jeffrey Gorsch	Vincent Jung
Michelle Nguyen	Michael Nguyen	David Tran
Art Nantasenamat	Tewodros Metaferia	

Reviewed by:

David H. Olwell Ph.D.
Chairman, Department of Systems Engineering

Released by:

Dan C. Boger
Interim Dean of Research

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 0704-0188
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188) Washington DC 20503.			
1. AGENCY USE ONLY ***(Leave blank)***	**2. REPORT DATE** September 2006	**3. REPORT TYPE AND DATES COVERED** Technical Report	
4. TITLE AND SUBTITLE: Implication of FORCEnet on Coalition Forces			**5. FUNDING NUMBERS**
6. AUTHOR(S) Naval Postgraduate School, Master's of Science in Systems Engineering, Port Hueneme Cohort 4			
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943-5000			**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A			**10. SPONSORING / MONITORING AGENCY REPORT NUMBER**
11. SUPPLEMENTARY NOTES: The views expressed in this report are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.			
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			**12b. DISTRIBUTION CODE** A

13. ABSTRACT ***(maximum 200 words)***

The coalition navies of Australia, Canada, New Zealand, United Kingdom and the United States (AUSCANNZUKUS) are in a period of transformation. They are stepping out of the Industrial Age of warfare and into the Informational Age of warfare. Network Centric Warfare (NCW) is the emerging theory to accomplish this undertaking. NCW describes "the combination of strategies, emerging tactics, techniques, and procedures, and organizations that a fully or even partially networked force can employ to create a decisive war fighting advantage." [1] This theory is turned into a concept through Network Centric Operations (NCO) and implemented through the FORCEnet operational construct and architectural framework. The coalition navies are moving in a direction to develop and leverage information more effectively and efficiently. This will lead to an informational advantage that can be used as a combat multiplier to shape and control the environment, so as to dissuade, deter, and decisively defeat any enemy.

This analysis was comprised of defining three TTCP AG-6 provided vignettes into ARENA model that captured Coalition ESG configurations at various FORCEnet levels. The results of the analysis demonstrated that enhanced FORCEnet capabilities such as FORCEnet Levels 2 and 4 would satisfy the capability gap for a needed network-centric ESG force that can effectively counter insurgency operations in Maritime warfare. Furthermore, the participating allied navies in the Coalition ESG should pursue acquisition strategies to upgrade their ship platforms in accordance with our recommendation which indicates that FORCEnet Level 2 is the best value.

14. SUBJECT TERMS			**15. NUMBER OF PAGES** 163
			16. PRICE CODE
17. SECURITY CLASSIFICATION OF REPORT Unclassified	**18. SECURITY CLASSIFICATION OF THIS PAGE** Unclassified	**19. SECURITY CLASSIFICATION OF ABSTRACT** Unclassified	**20. LIMITATION OF ABSTRACT** UL

[1] The Implementation of Network-Centric Warfare, Office of FORCE Transformation.

THIS PAGE INTENTIONALLY LEFT BLANK

CAPABILITY DEVELOPMENT DOCUMENT FOR COALITION FORCENET EXPEDITIONARY STRIKE GROUP (ESG) "IMPLICATION OF FORCENET ON COALITION FORCES"





Prepared for the Naval Postgraduate School (NPS)

Prepared by:

COHORT IV SI0810 ~ COALITION FORCENET TEAM
PORT HUENEME DIVISION, NAVAL SURFACE WARFARE CENTER
PORT HUENEME, CA 93043-4307
September 2006

THIS PAGE INTENTIONALLY LEFT BLANK

EXECUTIVE SUMMARY

The goal of this project was to provide an analysis of acquisition strategies of FORCEnet for coalition forces, provide an analysis of the architectural framework, provide an analysis of the operational benefits of FORCEnet for coalition forces, and provide guidance for the technical recommendations for the framework in support of naval coalition forces. The approach has taken into account the functional levels of interoperability, assessed the incremental values of the levels of interoperability, and provided input to the investment studies.

The premise taken into account has been that the forces of the future will be exposed to many different challenges. These challenges include new threats and declining economies, requirements to surge the forces outside of their normal deployment cycle, Ballistic Missile Defense, decreasing force structure, and new technologies.

Future naval forces will need to be coalition in nature to maintain a global force presence. Future coalition forces are anticipated to require Expeditionary Warfare requirements that provide a more robust and responsive suite of naval forces that:

- Provide expeditionary, multi-tiered sensor and weapon information
- Conduct distributed, collaborative Command & Control
- Provide dynamic, multi-path and survivable networks
- Provide adaptive / automated decision aids
- Provide Human-Centric Integration (HCI)
- Provide an Information Operations advantage

The forces will be required to maintain capabilities for:

- Shared planning & training capabilities
- Shared situational awareness
- Filtered, managed and load balanced bandwidth
- Distributed intelligence & information through voice, and network capabilities
- Common operating picture (COP) through synchronized network services
- Real-time, accurate & timely targeting information
- If required, fully networked weapons systems controlled by an approved authority

To evaluate the benefits of FORCEnet, the levels of FORCEnet were defined and then evaluated against options of procurement. These options were then modeled against naval scenarios in and around the Philippine Islands, employing AUSCANNZUKUS Coalition forces, and to study the Coalition impact of participating in the USN FORCEnet (Fn) program.

The framework for this study was derived from the Operation Philippine Comfort - CJTF scenario. The scenario is based around a natural humanitarian disaster (volcanic eruption) creating international sentiment which requires relief action on the part of each nation. Each AUSCANNZUKUS nation has naval and/or military assets in the area. The Philippine government is also experiencing political unrest due in part to separatist insurgency whose intent is to use the disaster as an opportunity to achieve their goal of further unrest and insurgency. The mission of the coalition naval forces is to ensure that disaster relief is not impeded by the previously covert, but now openly aggressive support of the separatists and their naval units by another Southeastern Asian nation.

The project provides a threat summary, operational environment summary, intelligence supportability, policy, rules of engagement, security levels, command /control architecture, operational architectural frameworks, DOTMLPF recommendations, modeling, financial summary and procurement recommendations.

The three phases of the Operation Philippine Comfort scenario were modelled using Arena, which is a general purpose, discrete event simulation environment. The software utilizes a visual programming paradigm to enable the straightforward construction of models, coupled with the flexibility of both general purpose and simulation specific programming languages. The phases modelled using four levels of FORCEnet and three options of implementation. The phases of the scenario modelled were 1) the Expeditionary Strike Group effectiveness with a surface warfare threat of an Indonesian surface action group, 2) the amphibious offload of support to the Philippine government, and 3) Naval fires support against a land based insurgent missile attack against the coalition naval forces.

The options analyzed were: Option #1 - Small size (all US) ESG force, fully Fn capable, Option #2 - Added Coalition ships, but not Fn capable (i.e., larger overall force),

Option #3A - Intermediate Fn capability to the additional Coalition ships, Option #3B - Intermediate Fn capability to the additional Coalition ships (addition of Fire Control Picture (FCP) quality data), and Option #4 - Full Fn capability to entire force.

The modelling showed a significant increase in the effectiveness between option 3A and option 3B of the ability of the coalition forces to maintain an up-to-date common operational picture. Additionally, higher FORCEnet levels facilitated the lead time in obtaining complete COP information, faster reaction times to threats and increased surveillance ability. Higher FORCEnet levels also enabled the increased ability for insurgent land attack suppression and threat destruction. The effectiveness between option 3B to option 4 resulted in a relatively minor increase in capability.

Financial analysis of the cost of entry and amount of life-cycle costs included R&D costs, acquisition costs, and operation and support costs. Given the effectiveness and the associated life-cycle costs it is recommended that the coalition partners would benefit from a spiral development acquisition and implementation plan. The costs increased in levels of FORCEnet for the coalition force units, as expected. However the associated costs between the levels of FORCEnet used in the options of procurement were approximately 40% higher between option 3B and 4, which was a higher increase than previous levels.

The project recommendation is that the coalition partners would gain the greatest operational and financial benefits by implementing option 3B within the procurement plan.

INTRODUCTION

Background

This paper follows a modified Capabilities Development Document (CDD) format as requested by our CAPSTONE Project Advisor and The Technical Cooperation Program (TTCP), Action Group 6 (AG-6). Our CAPSTONE project CDD format is consistent with Chairman of the Joint Chiefs of Staff, Operation of the Joint Capabilities Integration and Development System, CJCSM 3170.01B. The rationale for using the CDD format, as opposed to a traditional thesis format, is that the CDD format required a methodology that captures the necessary details of FORCEnet such as to identify existing capabilities, capability gaps, concept of operations, projected threat environment, DOTMLPF considerations, modeling, and program affordability.

This CDD seeks to explore the implications of various FORCEnet implementation configurations for the United States and participating Coalition naval forces under as part of an Expeditionary Strike Group FORCEnet construct that we analyzed and modeled using an Operation Philippine Comfort Scenario study provided by TTCP, AG-6. The CDD comprises the results of analysis performed by students of the Naval Postgraduate School (NPS) in the Master of Science in Systems Engineering (MSSE) curriculum, and is thus presented from a Systems Engineering perspective. The students are currently employed by the Naval Surface Warfare Center, and work in varying capacities supporting the U.S. Naval Fleet. Our analysis was guided and supported by TTCP, AG-6. The outcome of this analysis presents the Action group TTCP members with a recommendation of what network-centric system attributes that should be considered for their continued national balance of investment studies. Overall, it was determined the CDD format would best lend itself to assist participating coalition partners to make a more informative decision into their FORCEnet investment strategies.

FORCEnet Background

The overarching theory of Net Centric Warfare (NCW) and the U.S. Navy's FORCEnet concept in particular, provide a vision of the future that promises both substantial change and significant opportunity. If coalition navies wish to improve, or even maintain, their existing capabilities for interoperating with U.S. naval forces, they must address the implications of this new paradigm to better prepare for that eventuality. One of the goals of NCW is a flattening of the lines of command. Ideally, all coalition forces would enjoy equal access to information. The reality of the current environment, however, is that some forces are more equal than others. In light of that reality, this paper will present a theme of "asymmetric collaboration."

Trade and technology are fundamentally altering our world. Individuals have unprecedented access to information, and the ability to travel to the ends of the earth, including those willing and able to harm U.S. interests. In spite of the global reach of terrorism, however, the local nature of many terrorist groups implies that coalition partners often possess the best means for providing actionable intelligence. We are as interdependent as ever, and becoming more so. And while this kind of environment can be expected to foster a reduced chance for major wars, future threats are likely to involve significant regional conflicts, non-state actors, and the need for Operations Other Than War (OOTW).

In parallel with the changing threat environment is the opportunity for enhanced warfighting through the application of modern information technology. This is the essential basis for NCW. These changes argue for more agile, flexible force structures, greater use of information technology, and greater cooperation between U.S. and coalition partners. FORCEnet is a potential enabler for all of these goals.

Importance of FORCEnet Implementation

The "fog of war" has been a bane to commanders and warfighters for millennia. Information technologies present the possibility for dissipating, if not completely

eliminating this uncertainty. NCW theories posit a relationship between network connectivity and combat effectiveness via information superiority and shared situational awareness. The CONOPS for a FORCEnet enabled coalition thus incorporates a secure, robust, composeable, and highly coordinated network of both U.S. and coalition assets, including sensors, weapons, and Command, Control, Computers, Communication, Intelligence, Surveillance, and Reconnaissance (C4ISR) assets, that spans from "seabed to space and sea to land." Interoperability will be enabled via common technical standards, coordinated Tactics, Techniques, and Procedures (TTPs), integrated training, exercises, and operations, and access to distributed services, including resource management, collaborative planning tools, automated decision aids, and reach-back capabilities. Shared situational awareness will be facilitated by the distribution of a Common Operational Picture (COP), a Common Tactical Picture (CTP), a Single Integrated Air Picture (SIAP), and if bandwidth is sufficient, a common Fire Control Picture (FCP).[2] Data fusion techniques will enable increased tracking and targeting accuracy, and will accommodate asymmetric platform capabilities by decreasing network bandwidth requirements. The modeling and cost estimation analysis results outlined in our CDD will demonstrate the importance for our Coalition partners in continuing pursue FORCEnet technologies that that will facilitate an optimized network-centric capability that is needed to enhance Coalition ESG maritime operations.

Desired Capabilities / Capability Gap

In Section 1 of the CDD, our group presents a capability gaps discussion that describes the minimum desired capabilities for coalition platforms which include the ability to link into U.S. networks, contribute to a COP/CTP, and to coordinate surface, subsurface, and/or air operations. The capability gaps are derived from description of the intended Coalition FORCEnet ESG environment described in the Concept of Operation (Section 3, CDD) and the projected enemy threat (Section 4, CDD) Additional desired

[2] Summarized from "Naval Network-Centric Sensor Resource Management," Bonnie Worth Johnson and John M. Green

capabilities include providing information transfer, network protection, and deployable ISR assets, sharing ISR data across the force, and participating in mission planning.[3] Although most coalition partners possess at least some of these capabilities, they are unequally represented across the force, and are often only partially developed.

CDD Analysis Approach

In Section 2 of the CDD, a brief description of our group's analysis approach is presented. The scope of analysis captured was bounded by our terms of reference, as provided by MAR AG-6, which supplied a predetermined operational scenario and defined levels of potential capability. Within the scope of these parameters, we conducted both qualitative and quantitative evaluation. Qualitative analysis involved consideration of both architectural and cultural elements. Quantitative analysis consisted of both Agent Based Modeling (ABM) and affordability analysis. The operational scenario selected for analysis, "Operation Philippine Comfort," has been used as the basis for previous FORCEnet demonstrations. It involves coalition naval forces responding to a humanitarian crisis, and a gradual escalation of conflict.

Architectural Considerations

As part of our analysis, we additionally considered that FORCEnet is not a program of record, and unlike the Army's approach to NCW, does not enlist the efforts of a lead systems integrator. The ultimate effectiveness of FORCEnet therefore hinges upon the successful implementation of a system of systems approach, with the foundation of a standards-based Open Architecture (OA). Within this framework, individual coalition partners are free to develop systems and capabilities that are both tailored to their specific needs and compatible with U.S. forces. Key areas for the development of FORCEnet capabilities that we considered were composeability, information quality, and Information Assurance (IA).

[3] Summarized from Command, Control, Communication and Computer Intelligence Reconnaissance (C4ISR)," RADM Mark R. Milliken, Director, Navy International Program Office, May 18, 2004.

Cultural Considerations

As important as architectural considerations are, they are only a means to an end. Physical systems are ultimately used by people, and their characteristics are as important, if not more important, than the systems they operate. It is therefore best to view human and technical elements as part of a combined system. Only in this context does system performance have any true meaning. Among the human characteristics that distinguish between national components of a coalition force are those that could be considered cultural in nature. Cultural elements include doctrine, organization, training, leadership, and personnel. Effective implementation of interoperability requires alignment in all of these areas. In Section 12 of the CDD, we describe many of the cultural considerations as part of our Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities (DOTMLPF) analysis. A summary of some of the content as reflected in the CDD is as follows:

Doctrine is an established set of high-level principles that guide the actions of military forces. Current U.S. doctrine establishes the importance of both network-centric and coalition warfare. Without similar underpinnings among coalition forces, it will be difficult to make the changes necessary to support shared Network Centric Operations (NCO). Rules of Engagement (RoE) in particular will need to be constructed so as to maximize collaboration while maintaining national priorities. Command and Control (C2) doctrine will also need to adapt to address the decentralization and self-synchronization that are made possible by future network structures.

Organizational structures are another area in which change needs to be addressed. This is particularly true with regard to intelligence capabilities, which have not traditionally been horizontally integrated. Current U.S. doctrine dictates that horizontal integration will be implemented as a part of future systems to enhance collaboration and shared situational awareness. Force structures also need to adapt to an increased emphasis on littoral warfare and composeable capability packages.

Training both improves the effective use of NCO and is itself significantly enhanced by NCO. Changes in doctrine, RoE, TTPs, technical standards, and the introduction of distributed services will require the commitment of significant resources to the development of guidance and education. Fleet exercises as well are an important means for developing and practicing the tools necessary to implement net-centric collaboration. Trident Warrior is an excellent example of the potential benefits of these kinds of exercises. Ongoing collaborative programs, such as TTCP, are also important for developing the trust and rapport needed to foster better collaboration, and help develop a "network" of individuals who could interface in future exercises and operations.

Although FORCEnet will provide a broad suite of new tools for leaders to utilize, it will also require a number of new competencies. Balance must be struck between the increased need for collaboration and the capacity for increased speed of command that new networks will provide. Commanders need to be aware of both the capabilities and limitations of network-centric constructs, and to effectively utilize the decision aids made possible by distributed services. They must also be able to leverage the additional resources that coalition operations will make available to them. As with the future threat environment in which they will operate, leaders will be provided both challenges and opportunities. Future manning concepts will require a smaller cadre of well-educated and highly trained personnel that are comfortable with information technology and capable of collaborating with a wide range of potential coalition partners. The capacity for self-synchronization in particular implies an inherent need for highly skilled and proactive personnel. They must behave, in other words, more like leaders and less like subordinates. Better selection methods, as well as proper training can help in this regard.

Modeling

As reflected in Section 13 of our CDD, three phases of the Operation Philippine Comfort scenario were modelled using Arena, which is a general purpose, discrete event simulation environment developed by Systems Modelling Corp. (acquired by Rockwell

Software). The software utilizes a visual programming paradigm to enable the straightforward construction of models, coupled with the flexibility of both general purpose and simulation specific programming languages.

Measures of Performance (MOPs) were also determined that used a quantifiable means for evaluating the effectiveness, efficiency, timeliness, and risk associated with coalition FORCEnet implementation. The overall results of the modeling analysis against the defined MOPs are reflected in Section 13 of the CDD.

The Modeling results in the CDD will show that more FORCEnet technology enhancements is better. With only minor exceptions, higher levels of FORCEnet implementation resulted in consistently better performance. This result is tempered, however, by the realization that there are diminishing returns involved (this issue will be addressed within the context of the affordability analysis in Section 14 of the CDD)

.

Acquisition Approach / Affordability

In Section 14 of the CDD we show how the development of complex systems poses both cost and schedule risk. These risks can be mitigated by means of evolutionary acquisition methods, including spiral development. A spiral development model, with three notional phase increments, was explored as part of our cost analysis. Increment one would encompass development of a Maritime Tactical Wide Area Network (MTWAN) capability similar to that provided by the Combined Enterprise Regional Information Exchange System (CENTRIXS). Increment two would consist of an enhanced tactical data link capability similar to the Joint Tactical Radio System (JTRS). Increment three would provide enhanced networking capabilities similar to the Cooperative Engagement Capability (CEC).

Estimated Life-Cycle Costs (LCC) for the three different levels of FORCEnet capability were determined (results in graphical charts format are in Section 14 of the CDD). Although modeling results indicated that the highest level of FORCEnet implementation did demonstrate the best performance, it did not provide the most cost-effective capability. Because of diminishing returns, we determined that level two (Fn2) was more cost effective.

Recommendations / Conclusion

As part of our costs analysis conclusion in Section 14 of the CDD, our group developed the conclusion that is comprised of a tradeoff between a Fn Level II and IV implementation:

- FORCEnet Level 4 provides the higher performance
- FORCEnet Level 4 associated costs are higher
- FORCEnet Level 2 provides comparable performance levels at ~ 40% less cost than FORCEnet Level

The culmination of our Coalition FORCEnet analysis as presented in CDD format reflects key considerations and summary recommendations concerning the effective implementation of coalition FORCEnet capabilities as follows:

- Adopt a system of systems perspective and open standards; implement system requirements for composeability, information quality, and information assurance
- Implement a multi-tiered network architecture consisting of local networks as well as SATCOM links to shore-based networks; address latency issues as well as bandwidth; implement IPv6 to benefit from QoS protocols; implement data fusion methods
- Address IA from a systems approach, implementing robust, system-wide encryption methods, Cross-Domain Solutions (CDS), and defense-in-depth

- Pursue improved interoperability via common technical standards, coordinated Tactics, Techniques, and Procedures (TTPs), integrated training, exercises, and operations, and distributed services
- Implement appropriate changes relating to doctrine, organization, training, leadership, and personnel
- Mitigate cost and schedule risks through the implementation of an evolutionary acquisition strategy (spiral development); balance the relative costs and benefits of increasing levels of FORCEnet implementation at the beginning of each spiral, adjusting requirements as needed
- Pursue future studies in cognitive domain modeling, and quantifiable measures of required bandwidth

Although the challenges associated with its implementation are considerable, FORCEnet offers the potential to be a powerful force multiplier for both U.S. and coalition assets. With suitable preparation and the knowledge of its implications for coalition forces, the benefits of collaboration can be more fully recognized, and the promise of net-centric warfare more fully brought to reality.

Additional Considerations

In Section 15 of the CDD we present additional considerations for future NPS Coalition FORCEnet studies. Basically, we summarize FORCEnet as a broad and dynamic area of study, requiring careful consideration of a large number of specialized fields of knowledge. The completion of our analysis in the required timeframe thus required a significant scoping of our efforts; however, in Appendix C of the CDD, our CAPSTONE project group was able to conduct preliminary analysis of other vignettes from the TTCP Operational Philippines Scenario that could be leveraged by future NPS student in their continuing efforts with Coalition FORCEnet studies. Additionally, other areas of possible future study include cognitive domain modeling, data fusion methods, and quantifiable measures of required bandwidth.

TABLE OF CONTENTS

TABLE OF CONTENTS - CONTINUED

TABLE OF CONTENTS - CONTINUED

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

LIST OF FIGURES

1.0 Capability Discussion

1.1 Capability Gap Overview

While there is recognition that U.S. and Coalition navies must leverage network-centric technologies to achieve information dominance and maritime superiority, current capabilities fall short of achieving true FORCEnet objectives. As summarized in a recent TTCP Technical Report, "Specific technical issues like bandwidth constraints have been raised as imposing significant limitations on the success of coalition FORCEnet."[4]

Given that the overall goal of FORCEnet is to "integrate warriors, sensors, networks, command and control, platforms and weapons into a networked, distributed combat system force, scalable across the spectrum of conflict from seabed to space and sea to land,"[5] U.S. Naval forces must continue to pursue acquisition goals for enhanced FORCEnet capabilities in addition to providing allied forces with the necessary technologies and network links that would characterize a formidable coalition navy operating in the 2010 – 2015 time frame.

FORCEnet uses information superiority by establishing and maintaining shared awareness across the battle force. Information superiority provides battle force information that the Coalition Partners use to create clear, high quality Common Operational, Common Tactical, and Fire Control Pictures to shape and control the environment to dissuade, deter or decisively defeat the enemy. Given the Navy's recent efforts to procure FORCEnet technologies such as CENTRIXS, INMARSAT, GPS, C2PC and GCCS-M, current Coalition architectures have yet to be fully capable to operate in the FORCEnet domain. "Failure of coalition partners to attain the same level of composability as their U.S. partners could affect the efficacy of a future force."[6]

[4] Interpretation of TTCP MAR AG-1 Network Centric Warfare Study Tools and Results in Terms of the FORCEnet Construct, TTCP Technical Report, Dec. 2005, 5.

[5] Ibid, 20.

[6] Ibid, 7.

Networking

The use of varying communication standards does not allow the Coalition Partners to share tactical information, courses of action information, enemy order battle information, or fire control quality data efficiently or effectively to utilize the benefits of FORCEnet. The current Coalition Partners networks also lack the necessary bandwidth to handle or quickly transfer this data to each another. Improvements in standards and bandwidth are essential in the Coalition Partners network to realize a COP, CTP, and FCP to provide an information superior advantage.

The first step in achieving an integrated Coalition network is to solve the issue of Coalition Partners operating different communication standards, such as Link-11, Link-16, Satellite Link-16, Link-22, and the NATO Improved Link Eleven (NILE). By solving this issue, Coalition Partners will be communicating on a single tactical data link standard and will achieve a common required throughput, granularity, and extended ranges to quickly share information within the battle space.

Weapons and Sensors

The Coalition Partners situational awareness space and engagement space is limited in sensor range capabilities and weapon engagement range capabilities. Weapons and sensors are critical in gaining battle space superiority. The Coalition Partners are improving the sensor and engagement grids with the use of new technologies like the Cooperative Engagement Capability (CEC) and Joint Range Extension Application Protocol (JREAP). However these methods have their limitations in range, bandwidth, and information sharing capabilities.

Coalition Partners' sensors are platform centric and need to be integrated and synchronized to achieve network-centric capabilities. The desired goal is to derive the optimum balance of sensors to weapons systems required to generate timely and accurate fire engagements. Integrating sensors in a network-centric manner would provide an improved quality FCP and COP to effectively extend the envelope to maximum weapons range.

Command and Control

The command and control that the Coalition Partners utilize is not designed to perform in a network centric environment. The current set up is a platform centric architecture that is non-collaborative, independent of other platforms, and stove-piped. This architecture does not allow sensors to integrate to provide greater separation to increase and improve surveillance space. The Coalition Partners need an architecture with the ability to share local data and processed information with all battle force nodes, provide continuous automated information sharing, and share battle force resource commands.

Currently, the Coalition Partners are unable to collaborate to achieve coordinated resource management. The Coalition Partners need a decentralized framework that will be able to share an identical tactical picture. The various current platforms and platform-centric architecture makes it impossible to form composite tracks. The coalition partners will require methods for providing high-speed data fusion at a minimum for data deconfliction and synchronization.

1.2 Addressing the Interoperability Capability Gap

In "TTCP Technical Report," dated December 2005, it was recommended that the FORCEnet interoperability capability gap be addressed "by moving to study the impact of a particular instance of a particular network enabled construct, the U.S. Navy's FORCEnet, on coalition navies"[7].

The forces of the future will be exposed to many different challenges. These challenges include:

- New threats and declining economies
- Requirements to surge the forces outside of normal deployment cycles
- Ballistic Missile Defense

[7] "Interpretation of TTCP MAR AG-1 Network Centric Warfare Study Tools and results in Terms of the FORCEnet Construct", TTCP Technical Report by Subcommittee on Non-Atomic Military Research and development, December 2005.

- Decreasing Force Structure
- New Technologies

The combination of challenges over several different areas of operations and possible scenarios will be more than any single national naval force can sustain for any period of time. The forces of the coalition nations will be needed to counter these challenges as they arise. As the coalition naval forces must be able to operate together upon a short notice, this requires that they are compatible in the types of procedures, equipment, and communications systems to be able to maintain a cohesive and superior force presence.

FORCEnet is a structure that the U.S. Navy has brought forth as a means for coalescing the means of communications with its naval forces. Using this same capability has been suggested for the coalition partners.

FORCEnet as a means for coalition communications would provide an advantage. However, with the advantage comes a cost of adding equipment, the task of defining the structure, the task of defining procedures, etc.

The coalition naval forces may not require a full suite of equipment to accomplish the task; however the challenge is to find the point on the curve where the investment provides the optimum combat capability.

The overarching hypothesis of the FORCEnet Functional Concept states "… that if all forces and organizations down to the level of individual entities are interconnected in a networked, collaborative command and control environment, then all operations and activities can enjoy the benefits of decentralization, including initiative, adaptability and increased tempo, without sacrificing the coordination or unity of effort typically associated with centralization."[8]

The operational impact should be "… command and control characterized by shorter decision cycles that allow commanders to make and implement better decisions faster than any enemy can tolerate…."[1] The results will be units and platforms able to

[8] "FORCEnet: A Functional Concept for the 21st Century," The Chief of Naval Operations, Admiral Vern Clark, and the Commandant of the Marine Corps, General Michael W. Hagee,

adapt more quickly and effectively to changing circumstances and the ability to self-synchronize in furtherance of the mission.

For the operational impact of FORCEnet command and control concepts over coalition forces, C2 must be analyzed and evaluated through scenario analysis (including operational analysis and financial analysis) to assess FORCEnet in quantitative and qualitative terms.

Analysis of collected data provides insights resulting in dedicated procurement and development decision information required to produce "speed to capability" (S2C). Speed to capability is the rapid fielding of improved FORCEnet C2 warfighting capabilities to the fleet with full supportability, maintainability, tactics, techniques and procedures.

In today's global war on terrorism with responses ranging from large or small scale regional conflicts to relief operations, there is a potential for the configuration of an expeditionary strike group (ESG) to include coalition partners pulled from their national regional assets. FORCEnet concepts must also provide continuity across the coalition with a Combined Forces Maritime Component Commander (CFMCC).

Key enablers of FORCEnet capability required to make the CFMCC fully capable of creating coalitions able to meet all challenges are:

- Naval Networks - Optimizing communications bandwidth on naval networks for the fleet and providing communications interoperability capability for coalition forces.
- Cross Domain Solutions (CDS) - Cross Domain Solutions create a network-centric capable strike group across U.S. and coalition forces. The technical means to include and increase the capabilities of the assigned staffs and ships from the coalition nations will need to be addressed. Specifically, CDS will need to address multinational, multilevel, multidomain and interoperability issues that involve dynamic networks consisting of guards that support cross domain transfer of information.

- Information Management/Collaboration - This is essential to create and manage a CFMCC information management plan that addresses information management and processing between coalition units brought together in an ESG.
- Command and Control - C2 decision tools are essential to synchronize planning and resource management for assets across the strike group. CFMCC operational planning tools and a common operating environment (COE) that integrates access to data used in automatic generation and dissemination of maritime task plan information will need to be developed.
- Intelligence, Surveillance and Reconnaissance (ISR) - Future synchronization of ISR capabilities will be worked through distributed ISR nodes, which, in turn, will support effects-based operations in joint-coalition environments. ISR will bring interoperability and information exchange between Network-Centric Collaborative Targeting (NCCT) and Cooperative Engagement Capability (CEC) like products which are used to provide improved battle space awareness.
- Naval Fires - Automation through FORCEnet implementation of machine to machine (M2M) technologies enables movement of targeting information between aircraft and C2 nodes. This brings aviation assets into the Navy's fires process and provides the CFMCC with an increased ability to apply force within the battlespace.
- Information Operations (IO) - Information Operations are conducted using a variety of tools, all of which need to be coordinated and synchronized.

1.3 Operating Environment

The operating environment required for our analysis was provided by TTCP AG-6 and required analysis of a Coalition Expeditionary Strike Group configured in various FORCEnet level architectures operating in the littoral region in a Maritime Warfare Environment. This CDD will focus on three vignettes as part of an overall Humanitarian Aid and Disaster Relief (HA-DR) scenario set in the Philippines region. These three vignettes define operating environments characterized by ASuW against a Surface Action

Group threat, ISR coordination and monitoring of sea and land threats during amphibious offload, and Naval Surface Fires Support for amphibious offload operations.[9] Appendix C of this CDD also reflects our group's preliminary analysis of other vignettes for other operating environments (Assembly, Transit, Anti-Surface Warfare against Kilo threat, Anti-Air Warfare, Anti-Ship Missile Defense and Military Interdiction Operations). This preliminary analysis was conducted to assist future Naval Postgraduate students to continue Coalition FORCEnet studies.

The Coalition ESG forces will be comprised of US Naval Forces (one LHD, one LPD, one LSD, two DDG's, one CG, one SSN, and three LCS's) establishing a FORCEnet architecture implementation for incorporating allied navies (Canada – one FFG, one DDG; Australia – one FFH, one FFG, one AWD; United Kingdom – one FFG; and New Zealand – one FFH). Operating in the littorals of a Philippine maritime warfare environment, this Coalition ESG will be required to maintain and/or improve capabilities in the operating environment for:

- Shared planning & training capabilities
- Shared situational awareness
- Filtered, managed and load balanced bandwidth
- Distributed intelligence & information through voice, and network capabilities
- Common operational picture (COP) through synchronized network services
- Real-time, accurate & timely targeting information
- If required, fully networked weapons systems controlled by an approved authority

2.0 Analysis Summary

In order to analyze various alternatives to support a decision for coalition navies to participate in a U.S. Navy FORCEnet architecture, this Capabilities Development Document captures an analysis of a combination of various FORCEnet levels coupled with various configurations of a US and Coalition Navy ESG. As recommended by AG-

[9] Primary and preliminary analysis vignettes summarized from *Operation Philippine Comfort Scenario* Coalition FORCEnet Study, V0.g, 20 Jan 06, Jan. 2006.

6, a low-level operations analysis of a number of vignettes would be performed to provide the appropriate FORCEnet level for the coalition navies. This analysis comprises a Systems of Systems approach that projects various levels of FORCEnet capabilities that are fed into a model of the different vignettes. MOEs and MOPs are defined to assess the modeling results. A cost analysis was also completed to determine the cost of entry of allied navies into a US FORCEnetted network.

3.0 Concept of Operations Summary

The projected Coalition FORCEnet operational concept is comprised of an integrated architecture of U.S. naval platforms with coalition assets, joint assets and national assets as reflected in Figure 1 OV-1. Other integrated architecture products for our analysis are listed in Appendix A. Coalition FORCEnet will interface with various space, air, and land platform nodes creating an integrated situational awareness picture. While utilizing the available network interfaces, a Coalition ESG under a FORCEnet construct is effectively able to generate and maintain a timely and accurate COP, CTP, and FCP that will leverage the necessary information dominance over threat forces.

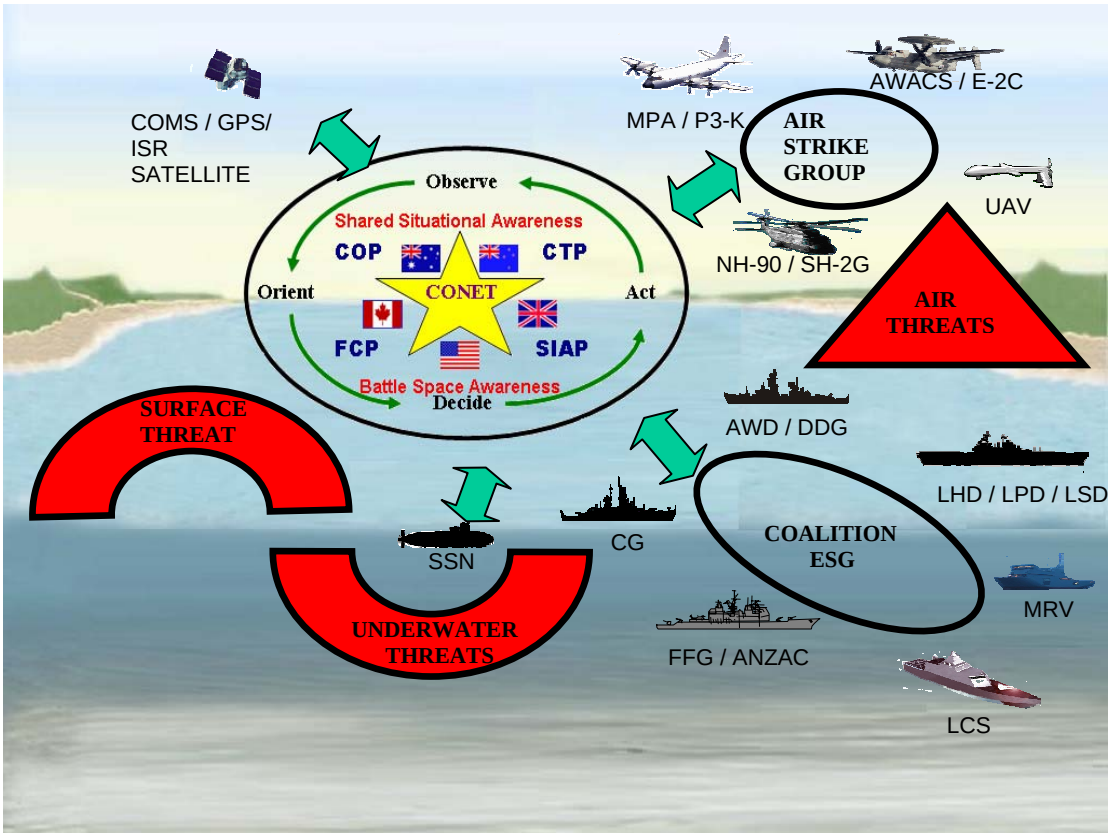


Figure 1. OV-1 Coalition FORCEnet

The concept of operations for coalition forces in the year 2010- 2015 will continue to include frequent training, exercises and common operations. Coalition forces will therefore be projected to utilize similar references and procedures. Because of the dispersed and decentralized nature of the future battle space, an ESG enhanced within a network-centric environment will meet the demands for an integrated force to effectively perform mission in joint, combined, and coalition operations.

As the CFMCC, the senior officer of the coalition forces will be designated as the officer in charge of the forces (see Figure 2). The officer in charge will be referred to as Alpha Bravo (AB). The coalition forces will be characterized with a distributed warfare area construct. The officer in charge can be expected to designate commanders of the most capable units as the designated warfare area commander. Warfare area commanders will then promulgate commanders' intentions to other units in the force. The air warfare commander will be designated as Alpha Whiskey (AW). The surface warfare

commander will be designated as Alpha Sierra (AS). The sub surface warfare area commander will be designated as Alpha X-ray (AX). The maritime interdiction warfare area commander will be designated as Alpha Mike (AM).[10]

[10] Description of Warfare Area command designations from Naval Warfare Publication NWP 3-56, Navy Warfare Development Command.

Warfare Area Organization

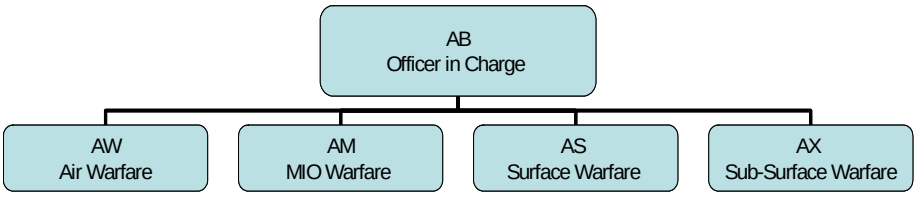


Figure 2. Warfare Area Organization

Coalition forces will be familiar with FORCEnet tools, procedures and include the use of all resources available. The resources shall be used for communications, planning and tactical awareness. Tactical awareness shall collectively include the Common Operational Picture (COP), Common Tactical Picture (CTP), and Fire Control Picture (FCP). Overall, the utilization of FORCEnet resources in the future maritime battle space will provide the ESG and coalition forces with the necessary tools to successfully operate in widely dispersed operational areas. It will also allow them to meet the demands for timely data/target processing through decentralized execution in a suite of networked platforms.

Communications will consist of a coordinated combination of RF, Satellite and Laser Line of Sight communications. The battle group commander shall issue a standard communications plan that designates which circuits shall be used for the different warfare areas. RF communications shall include HF, SHF, UHF, EHF line of sight, over the horizon and satellite voice communications circuits. Communication circuits shall be

encrypted using common encryption ciphers changed periodically[11]. Circuits shall include voice and digital data using time division multiple access (TDMA) technology. Laser high-speed data links may be considered for secure line of sight transmission.

Advanced tactical data links capabilities shall be used for tracking, correlation, intelligence gathering, and target ID. Tactical Data links shall be used to promote a more timely and accurate COP and CTP. Less capable units shall transmit to more capable units, which shall act as fusion nodes, which will collect and translate between the units.

Fire control quality data will be transmitted using enhanced cooperative engagement capability (CEC) like capabilities. Fire control quality data shall be used for more accurate and timely weapons engagements. Resource managers shall use this data as well to implement optimal weapons to sensor pairing and expedite engagements using automated decision aids that reflect the Commander's Guidance to include limitations imposed by specified rules of engagement.

4.0 Threat Summary

A potentially formidable threat against a networked coalition is one that is characterized with having the capability to impose an effective network or electronic warfare effort against a FORCEnet ESG. The intent of this type of attack would be to disrupt the communications and data sharing capability of the coalition partners. Examples of the objective of these attacks are loss of one of the communication nodes, denial of service or disruption of the quality of service. Spoofing and disinformation would also be attempted. The solution suggested here is to maintain a robust enough network capable of detecting and withstanding these types of threats while maintaining the connectivity and quality of service required for conducting operations.

As described in the provided "Operation Philippine Comfort Scenario Comfort Study"[12] it is predicted that Southeast Asian forces will possess these electronic warfare

[11] Description of RF communications from DODD 4630.5, 5 May 2004, "Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS)."

[12] Characterization of the Indonesian naval and insurgency threat is summarized from *Operation Philippine Comfort Scenario* Coalition FORCEnet Study, V0.g, 20 Jan 06, Jan. 2006.

capabilities along with an aggressive information warfare campaign to promote the insurgency effort. In addition to protecting against electronic and information warfare efforts pursued by the threat, the FORCEnet ESG still has to confront the vast suite of enemy platform threats (ships, attack boats, submarines, and insurgents on ground) and be successful in dominating them to achieve and sustain maritime superiority.

The armed forces of several Southeast Asian nations are a significant force in the region, representing a potential threat to the Philippines. A notional Southeast Asian naval force consists of 2 Kilo SS, 8 Parchim Corvette[13], 6 Fatahilah Corvette, 3 Van Spijk Frigate, 4 Kihajar Dewantara Frigate (non-operational), 12 Patrol Boat PSK-M, and 3 Tacoma LST.[14]

The Kilo SS is a quiet submarine equipped with 8 Strela-3 (SA-N-8 Gremlin) and 18 VA-111 Torpedoes. The Kilo Class was designed for anti-submarine and anti-ship warfare in the protection of naval bases, coastal installations and sea-lanes, and also for general reconnaissance and patrol missions. The Kilo is considered to be one of the quietest diesel submarines in the world.[15] The Parchim Corvette is an advanced patrol ship with anti-submarine capabilities. The Corvette is armed with 2 quadruple SA-N-5 (24 missiles), 2 twin 16-in torpedo tubes (400-mm), and 4 KH-35. The Fatahilah Corvette is a fast and small size anti-submarine ship equipped with 2 twin 16-in torpedo tubes (400-mm). The torpedo tubes can deploy 24 mines and are designed for firing remote-controlled torpedoes with a very high accuracy.[16] The Van Spijk Frigate is a multi-purpose ship that can be used in the anti-submarine, anti-aircraft, or surface combat roles. The primary armament consists of one 76 mm gun and 8 SS-N-14 ASCM that has both anti-ship and anti-air capabilities. The Patrol Boat PSK-M is a modern fast patrol boat equipped with four KH-35s with capability of cruising at high speed. The ship's design allows it to access very shallow water denied to other vessels, making it very littoral for close range attack. The Tacoma LST, equipped with 2.50 caliber gun, has

[13] http://en.wikipeida.org/wiki/List_of_ship_classes_of_the_Bundesmarine_and_Deutsche_Marine - accessed 7/02/06.

[14] http://www.globalsecurity.org/military/world/indonesia/alri.htm - accessed 6/24/06.

[15] http://en.wikipedia.org/wiki/Kilo_class_submarine - accessed 6/24/06.

[16] http://www.queocities.com/~uwezi/ships/parchim.html - accessed 8/01/06.

capabilities to transport and deploy troops, vehicles, and supplies onto foreign shores to conduct offensive and invasive military operations. [17]

The threat of maritime forces against the Philippines, especially when there is the overall disruption leading to a political crisis and government instability caused by the natural disaster of two large volcanic eruptions, in the southern Philippine islands is perceived as real.[18] Thus an accurate and comprehensive understanding of the threat is paramount. Due to the complexities of operating within the maritime domain and the unpredictable nature of the marine environment, attacking targets either on land or at sea by the enemy forces will be analyzed into specific tactical situations and broken into various vignettes as described in section 6c.

4.1 Operational Environment

The operational environment for this project calls for a scenario that introduces a wide range of asymmetric operations that will rely on a robust and dynamic FORCEnet force. In this case, an ESG under a network-centric construct would have to operate in a maritime operational area with the potential of a small attack boat threat while monitoring the advance of enemy naval surface threats, localizing the formidable enemy Kilo submarines, AAW and/or ASMD threats, performing amphibious offload to support countering of land-based insurgency, provide naval fires support, and conducting Maritime Interdiction Operations to prevent/hinder insurgent reinforcements.

The operational environment is further characterized with a need for dynamic reconfiguration of forces in response to close monitoring of the developing friendly and enemy situation. Decisions will have to be "powered down" to individual platforms that have the ability to responsively engage time critical targets or pass timely enemy information to other networked platforms such as to allow an effective collective response.

---

[17] http://www.hazegray.org/worldnav/asiapac/indones.htm - accessed 6/24/06.

[18] Characterization of the instability due to natural disaster is summarized from *Operation Philippine Comfort Scenario* Coalition FORCEnet Study, V0.g, 20 Jan 06, Jan. 2006.

The specific region for this project is defined in the Philippines region during which radical Islamic groups leveraged a natural disaster of two volcanic eruptions to create instability in the lower region in Mindanao. It has well been known that several Southeastern Nations are home to a number of militant Islamic groups. These include the Abu Sayyaf Group (ASG), which is based in the Philippines, the Free Aceh Movement (GAM) in Aceh, Indonesia, Jermaah Islamiyah (JI), which primarily operates from Indonesia, and the Moro Islamic Liberation Front (MILF) based in Philippines. The Al-Qaeda network is also believed to have established a presence in the region following the destruction of its bases in Afghanistan. All of these groups are known to use the maritime environment for logistical purposes, have developed maritime capability or have made preliminary steps toward acquiring capability in this area.

4.2 Information Operational Threats

With more emphasis in Information Operations as a combat multiplier for military forces, the coalition navies must sustain the information operations military advantage through it's participation in a US Navy FORCEnet implementation. Through projection of many regional threats as described in Section 4.0 "Operational Environment", one can expect formidable threats that can counter with effective information operations warfare. The US and Coalition Navy FORCEnet must provide a means of achieving information dominance in these various regions. A robust and secure network characterized with providing the right information at the right time will be required to maintain the information operations advantage over threat forces. Coalition forces must have the capability to quickly organize and dynamically link into a network that provides an exponential aggregation of sensors, C2 nodes, and weapons. Coalition platforms also must contribute to and receive critical situational awareness data that provides a timely and accurate COP, CTP, and FCP that facilitates an information operations advantage.

4.3 Threat Capabilities to be Countered, Threat Tactics

Projected threats can be expected to impose a disruptive network and electronic warfare capability characterized with the intent to disrupt and/or disable the Coalition FORCEnet network and communications. A Coalition FORCEnet must be able to implement an aggressive counter network/electronic warfare means to reduce the threat's effectiveness in this area. The potential vulnerability of the Coalition ESG in network-centric operations against interception and interference by technologically sophisticated adversaries is real and must be taken into account in developing FORCEnet architectures. Advances in intrusion detection capabilities must also be a part of the FORCEnet implementation along with affording the coalition navies with the same capabilities once integrated into the network. Security management, encryption techniques, login protections, and controlled information access of all FORCEnet participants must be embedded in the FORCEnet architecture.

5.0 Program Summary

The program should be developed in spirals. The purpose for breaking the development and fielding into spirals is to procure and field those systems which are easily integrated into existing systems and bring highly beneficial capability to the coalition.

The spirals are envisioned to be broken into three separate spirals. The first spiral would entail incorporating command and control capabilities through a CENTRIXS like capability. These options are 'low hanging fruit' which can be implemented quickly for a moderate to low cost. The second spiral can implement a tactical data link enhancement capability and enhanced communications (IP and Voice Over IP) capability. The third spiral can be used to develop and field a CEC like capability and implement enhanced network connectivity into the weapons systems for command authority engagements.

Breaking the implementation down into 3 spirals or phases as reflected in Figure 3 has the following advantages:

- Brings initial capability to the Coalition forces quickly

- Allows engineering activities to leverage off of previously resourced R&D efforts
- Allows engineering activities to implement lessons learned
- Allows for the enhancement of processes used for FORCEnet tools
- Distributes investment required for desired capabilities

Program Summary

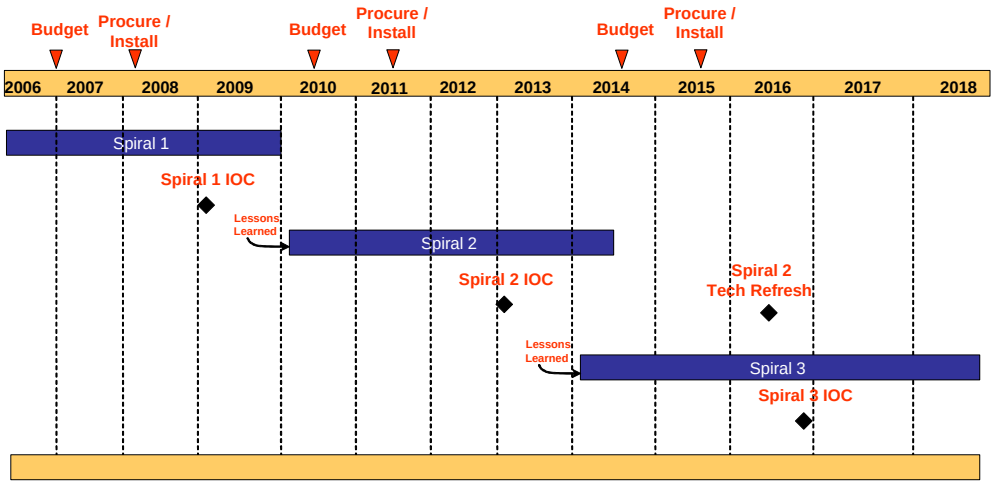


Figure 3. OV-1 FORCEnet Spiral Development Schedule

6.0 System Capability Comparison between FORCEnet Levels of Systems.

In modeling five different Coalition ESG options against three vignettes for this analysis, we identify and define the differences in the FORCEnet levels to be considered in the option configurations and how these differences are used to measure system effectiveness. The various FORCEnet levels to be considered for Coalition platform implementation are as follows:

(1) FORCEnet Level 0 - Current package of material solutions comprised of voice radio and capabilities similar to Link 11/16 to share situational awareness and Command and Control (C2) data. This solution is further characterized as platform-centric with local area networks, wideband receive, RF management, and survivable communications.

(2) FORCEnet Level 1 - Package of material solutions comprised of a coalition architecture with interoperability capabilities, improved bandwidth with higher fidelity/faster updates, reach back capability with broad distribution for data sharing, and ruggedized networks for improved security. Capabilities similar to CEC and tactical data link enhancements which allow wide data distribution (with some time delay) for networked platforms. An improved situational awareness picture is provided to all platforms with some minor time delay.

(3) FORCEnet Level 2 - Package of material solutions comprised of improved coalition architecture with interoperability capabilities that also include enhanced real-time targeting gained from any U.S. or coalition asset/source. This approach is similar to FORCEnet level 1, but with enhanced situational awareness characterized by good information accuracy, timeliness and coverage continuity. A major improvement with this level is the addition of an available Fire Control

Picture (FCP) for networked platforms that provide accurate and timely track and targeting information.

(4) FORCEnet Level 3 - Package of material solutions comprised of improved coalition architecture with interoperability capabilities that also include enhanced real-time targeting gained from any U.S. or coalition asset/source. This approach is similar to FORCEnet level 2, but with full bandwidth capabilities, redundant paths, and a common enterprise infrastructure. FORCEnet Level 3 would retain the same enhanced situational awareness picture as described in level 2. A major enhancement with this material approach is the availability of networked weapons systems into a more robust sensor to shooter grid; however, weapons availability is limited to within the established national networks as weapons control is by national authority. FORCEnet Level 3 with the addition of networked weapons systems offers an expanded FCP beyond what is described in FORCEnet level 2.

(5) FORCEnet Level 4 - Package of material solutions comprised of an optimum coalition architecture with fully netted interoperable capabilities. This material approach provides for all weapons systems available within the coalition forces. FORCEnet Level 4 provides the best situational awareness pictures to promote the best FCP for all coalition networked platforms. It will also provide a FORCEnet architecture that accounts for the necessity to screen out any sensitive data to coalitions platforms.

A more detailed description of FORCEnet capabilities based TTCP AG-6 efforts is located in Appendix B.

System capability comparison was performed using information from the SOW, “Operation Philippine Comfort” Scenario, guidance from NPS advisors and AG-6 members during an initial IPR briefing, and the defined AG-1 Key Performance

Parameters (KPP). The various option configurations that will be fed into the Arena model are as follows:[19]

Option	Description	Map to Benefits in Table 2
I (do nothing)	Small size (all US) ESG force, fully Fn capable	US part (level 3) No Coalition
II (do minimum)	Added Coalition ships, but not Fn capable (i.e. larger overall force)	US part (level 3) Coalition part (level 0)
III A	Intermediate Fn capability to the additional Coalition ships	US part (level 3) Coalition part (levels 1)
III B	Intermediate Fn capability to the additional Coalition ships	US part (level 3) Coalition part (levels 2)
IV	Full Fn capability to entire force	US and Coalition Units (level 4)

Table 1. Coalition FORCEnet Modeling Options

The scenario included eight mission areas defined in vignettes during which simulation was used for three of the vignettes (ASuW, Amphibious Offload, and Naval Fires Support) to determine which combination of materiel approaches provides the best coalition FORCEnet response.

Measures of performance applicable to modeled vignettes have also been identified as follows:[20]

[19] Options defined in Coalition FORCEnet Study, " Operation Philippine Comfort Scenario"

[20] MOPs derived from Coalition FORCEnet Study, " Operation Philippine Comfort Scenario"

Measures of Performance	Description
MOP 3.1	Amount of time SAG within sensing range.
MOP 3.2	Efficiency of asset allocation for monitoring duty.
MOP 3.3	Maintain up-to-date COP
MOP 6.1	Time to complete amphibious offload.
MOP 6.2	Ability to co-ordinate ISR assets before offload to monitor sea and land threats.
MOP 6.3	Ability to co-ordinate ISR assets during offload to monitor sea and land threats.
MOP 6.4	Maintain up-to-date COP.
MOP 7.1	Number of rounds taken to suppress truck attack
MOP 7.2	Time taken to suppress truck attack
MOP 7.3	Number of trucks destroyed
MOP 7.4	Number of trucks escaped.
MOP 7.5	Accuracy of first round falls of shot.
MOP 7.6	Time taken from call to fire, to first round impact.
MOP 7.7	Time taken from first anti-coalition attack to first round impact.

Table 2. Measures of Performance

7.0 Family-of-Systems and System-of-Systems Synchronization

The proposed FORCEnet architecture for the Coalition platforms must be part of an overall system-of-systems approach that leverages ongoing efforts of US Naval Forces R&D efforts with Network-Centric Warfare. It is critical that enhanced C5I platforms used to implement FORCEnet will be driven by hardware and interface requirements from a system-of-systems perspective. A piecemeal approach to simply replace legacy

systems with an improved C5I node is not the recommended approach for implementing our proposed FORCEnet architecture for the Coalition forces. FORCEnet implementation must be driven by system-of-systems requirements that address requirements for links into an enhanced bandwidth network, common data message formats, common automated decision tools, and user configurable access System-of-systems engineering deals with planning, analyzing, organizing, and integrating the capabilities of a mix of existing and new systems into a system-of-systems capability greater than the sum of the capabilities of the constituent parts. It is a top-down, comprehensive, collaborative, multidisciplinary, iterative, and concurrent technical management process for identifying system-of-systems capabilities; allocating such capabilities to a set of interdependent systems; and coordinating the integration of all the elements of development, production, sustainment, and other activities throughout the life cycle of a system-of-systems. The overall objective for developing a system-of-systems is to satisfy capabilities that can only be met with a mix of multiple, autonomous, and interacting systems. The system-of-systems approach to FORCEnet implementation must include a mix of constituent systems may include existing, partially developed, and yet-to-be-designed independent systems. Systems-of-systems should be treated and managed as a system in their own right, and should therefore be subject to the same systems engineering processes and best practices as applied to individual systems.[21]

The consideration for FORCEnet system-of-systems engineering should include the following factors or attributes:

- Larger scope and greater complexity of integration efforts;
- Collaborative and dynamic engineering;
- Engineering under the condition of uncertainty;
- Emphasis on design optimization;
- Continuing architectural reconfiguration;

[21] Defense Acquisition Guidebook, Version 1.0, Oct. 2004.

- Simultaneous modeling and simulation of emergent system-of-systems behavior;
- Rigorous interface design and management;

A family-of-systems approach for FORCEnet will enable coalition platforms with a consistent implementation of improved capabilities across each of the sensor, C2, and weapons suites. The FORCEnet family of systems is basically a grouping of systems (weapons, sensors, C2 nodes) having some common characteristic(s) that provide the recommended level of FORCEnet capabilities. A family of systems lacks the synergy of a system-of-systems, but this approach ensures a consistent implementation approach for multiple coalition platforms required to link into a US provided NCW network.

As the defense budget declines and the cost of defense acquisition rises, acquiring FORCEnet capabilities across the Navy enterprise (shore commands, sea borne commands, activities, and support structure) makes for good business sense. Basically, it makes sense to invest in common systems rather than investing in many different solutions that are not interoperable with each other and therefore causing more problems and requiring further investment for fixes. Not only is this good for the Navy, but it is beneficial to the joint and coalition forces as well. There are inherent benefits to this methodology.

- The cost of acquisition for coalition navies would be lower. As more units are procured, the cost per unit declines because there is more of a discount on the materials and labor.
- Configuration management becomes increasingly easier as there are similar baselines to work from and therefore upgrades are easier to manage.
- The systems become more compatible within the platforms, the joint services, the coalition services and across the area of operations.
- Synchronization of systems becomes easier due to the similar protocols, software and timing.
- Software design and code re-use makes software development more affordable.
- The infrastructure required to manage the shore logistics and engineering activities can be reduced.

In the pursuit of achieving the goal of the family-of-systems, a decision must be made to do so. It is anticipated, as sometimes occurs in normal human behavior, that there may be some resistance to change.

In the world of spiral development, the three threads that should be acted upon to achieve the end goal would be communications, computers and tactical data links. By leveraging these threads and enforcing the family of systems and their associated standards, the end goal may be easier and faster to achieve than if the task were attempted as one task.

As these spirals are developed, the family-of-systems should be engineered to the system-of-systems standards.

8.0 Intelligence Supportability

The Coalition ESG FORCEnet architecture will introduce enhanced intelligence supportability which is needed to improve ISR requirements. It is acknowledged by various allied navies that "The provision of timely and accurate intelligence to decision makers is a fundamental output of an effective NCW capability."[22] The US FORCEnet that will be available for allied navy's participation will provide the enhanced communication linkages to sea-based, aerial, land, and space platforms that will provide the timely and accurate intelligence data. Streamlined capabilities will be necessary to provide the right information at the right time to facilitate a military advantage in intelligence analysis necessary for an improved sensor to shooter grid.

8.1 Policies and Regulations

Given the sensitivity of intelligence data and assigned security levels based on the nature of the data, the Coalition FORCEnet will require the necessary unclassified and classified links that are accessible based on user platform needs and access control based on commander's guidance, joint operations policies, and national policies for each of the

[22] Australian Government Department of Defense, "NCW Roadmap" Chapter 8, October 2005.

allied navies. Participating nodes in a U.S. FORCEnet architecture will need to meet the regulations established for information technology accreditation that ensures all the necessary security protections are implemented.

Processing intelligence for potential engagements will be in accordance with specified rules of engagement policies. Rules of engagement will be promulgated by AB. Engagement orders and weapons postures will be transmitted by AB to the warfare area commander who will in-turn transmit to the individual units.

The rules of engagement are used as a basic guideline for the use of force within a hostile environment. All units will always have the inherent right of self-defense.

Hostile intent is defined as the clearly formulated plan or intention to commit an act of aggression which directly and deliberately interferes with operations of coalition forces, shows intent to do harm or inflicts bodily injury or death. Hostile intent includes but is not limited to directing weapons in a bearing towards coalition forces, use of continuous wave illumination or targeting radars on coalition forces, use of jamming against coalition forces radars and/or communication equipment, and firing of weapons at coalition forces. Contacts which continue on an inbound path and display hostile intent shall be warned.

Units will operate in a distributed architecture through command by negation, whereby the units will inform their warfare area commander of their intent and act accordingly. The warfare area commander's negation of intent will inhibit that unit from executing.

Strike Group Commanders will issue "Threat Warning Levels" to units within the strike group based on intelligence, surveillance and reconnaissance (ISR). The threat levels are a means for unit commanders to prepare their combat readiness levels.

<u>Threat Warning Levels –</u>

4: No perceived immediate threat exists to coalition forces.

3: A potential threat is possible to coalition forces.

2: A threat assessment indicates a threat to coalition forces exists and is credible.

1: A threat exists or an incident has occurred warranting the highest defensive posture.

Strike Group Commanders will issue “Weapons Posture Levels” to units within the strike group based on ISR, and/or recent developments within the area of operations. The weapons posture levels are a means for unit commanders to prepare and man weapons stations.

Weapons Posture Levels –

3: Weapons are maintained operational but not loaded or manned.

2: Weapons are loaded and minimally manned; ready to use upon notification.

1: Weapons are loaded, ready to fire and fully manned.

Strike Group Commanders will issue ”Weapons Levels” to units within the strike group based on ISR, and or recent developments within the area of operations. The weapons levels are a means for unit commanders to operate defensive and offensive operations.

Weapons Engagement Levels –

3: No weapons are authorized for offensive use in any warfare area.

2: Weapons are authorized for offensive use if a threat is positively identified as hostile.

1: Weapons are authorized for offensive use on any non-friendly unit. Contacts that have been designated as hostile shall be prosecuted without required permission.

Rules of Engagement Failure

The overall goal is to use forces effectively to accomplish the mission objectives and to avoid unnecessary force. However, during achievement of this goal, there is a possibility of creating the two following types of errors.

Type I: Excessively tight ROE which can constrain mission performance.

Type II: Excessively loose ROE which negates the political objectives that the forces try to achieve.

8.2 Security Levels

In consideration of information flow security under a Coalition ESG FORCEnet implementation, there must be a means to appropriately tag sensitive data and distribute it to select platforms based on a "need to know" basis. The FORCEnet systems must be able to provide multi level security access based on the data classification, authentication methods for transmit and receipt of data, and maintaining data integrity throughout data distribution (the intended message sent is the same message received). To facilitate Coalition platforms linkage into the US FORCEnet, appropriate system interfaces that filter data based on needs and security levels must be implemented in the Coalition FORCEnet architecture. Security requirements will be further enhanced by requiring unique user/platform logins for FORCEnet platforms. Resource managers will have awareness of all data requirements within the Sensor, C2, and Weapons grids and will ensure the timeliness of data distribution while maintaining security requirements.

8.3 DoD Information Technology Security Certification and Accreditation

Consistent with the Department of Navy's push for IT-21 certification for information systems, the same requirements will be imposed on future information systems under the FORCEnet construct. Stringent information assurance requirements as agreed to by US and Coalition nations will be met through implementation of security architectures as part of the overall FORCEnet architecture. These architecture components will include firewalls; virtual private networks; multilevel security; intrusion detection; synchronous optical network (SONET)/asynchronous transfer mode (ATM) security; secure Web protocols such as secure socket layer (SSL); virus detection; some authentication in routing, switching, and domain name service; and mail guards.

9.0 Electromagnetic Environmental Effects and Spectrum Supportability

A major concern in implementing a systems-of-systems solution as part of a FORCEnet package upgrade for Coalition platforms is ensuring the interoperability of all installed information, sensor, and weapons systems such that they do not degrade in performance due to electromagnetic effects. Projecting the utilization of COTS and the implementation of a commercial-like enterprise system as part of the FORCEnet solution, all systems must be designed and installed such as to avoid the potential concerns of electromagnetic effects that could degrade the performance of a Coalition FORCEnet platform. Proper shielding of hardware and cables is a must to survive in an electromagnetic environment. It is not anticipated that spectrum supportability will be an issue given the heavy reliance on external communications to drive the FORCEnet communications connectivity.

10.0 Assets Required to Achieve Initial Operational Capability (IOC)

The assets required for Initial Operating Capability (IOC), are minimal in comparison to the tasks required for IOC. The assets required are broken down into three different areas as follows:

- Command and Control: Capability similar to existing CENTRIXS units for each unit within the coalition force (IP based)
- Tactical Data Link: Capability similar to existing Link 22 for each unit within the coalition force (highly enhanced tactical data links)
- Communications: Capability similar to existing JTRS tactical programmable radio system

Using these three systems achieves a considerable amount of capability in the areas of command and control for initial operating capability.

Follow-on capability would require considerable investment into:

- CEC-like capability
- Enhanced networks and connectivity into combat systems, weapons and engineering networks.
- Communication bandwidth connectivity, including satellites and shipboard satellite antennas.

11.0 Schedule and IOC/Full Operational Capability (FOC) Definitions

The target date to attain IOC is based on a three spirals development schedule as described in Section 5 Program Summary (Spiral 1 – February 2009, Spiral 2 – February 2013, and Spiral 3 – November 2016). IOC for each spiral is satisfied when the intended FORCEnet capabilities are successfully demonstrated based on the pace of the spiral development. Ultimately, by spiral 3 a successful FORCEnet demonstration must allow a Coalition platform to use its sensors to detect a track, pass the track information to display within the platform, and forward the track information to another platform within the ESG. Successful communication must be verified on each participating platform with the minimum functionality as based on the recommended FORCEnet level to be implemented.

12.0 Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities (DOTMLPF) Considerations

12.1 Doctrine

Changes in doctrine will be required to account for the manner in which information is to be processed within the Coalition ESG. The new doctrine will have to reflect an operational philosophy based on maximum participation and the collaborative leveraging of capabilities in a network-centric environment. There will be streamlined paths for strategic tactical information data flow. New doctrine that addresses a more

geographically expanded operational area of influence for the Coalition ESG will have to be developed due to FORCEnet's information links into Joint and National assets. Additionally, issues associated with integration of allied platforms (i.e., commanders' guidance dissemination, weapons control, data filtering, dynamic platform configuration…etc.) will have to be integrated into doctrine to leverage FORCEnet capabilities for seamlessly expedient assembly and robust military planning for coalition operations. The doctrinal impacts due to Option 1 (US only Fn Level 3) and Option 4 (US and Coalition forces at Fn Level 4) implementation would require a minimal change in doctrine. Option 1 reflects the utilization of own country assets such as to maintain good C2 and tends to not incur significant doctrinal changes which would be needed for allied nation integration procedures. However, this most likely will not be the case for our future ESG deployments as we will continue to leverage allied nation's assets as part of US maritime warfare operation. Option 4 which contains allied nations at Fn Level 4 would provide the best bandwidth and network availability for data distribution and tracking doctrinal information (assignment of task organization, C2 relationships, commanders' guidance, fire support coordination measures, assigned boundaries,…etc.).

12.2 Organization

The implementation of a Coalition FORCEnet ESG would not be expected to have a significant impact on the organizational framework. The intent of a Coalition ESG under a FORCEnet construct is to establish the necessary command and control relationships through the help of decision aids and other automated tools, provide an ESG with a robust and flexible organizational structure to effectively execute a given mission with flexibility. Additionally, FORCEnet implementation can possibly drive a reduction in the number of needed platforms for mission execution, expanding the organizations area of operations/influence due to enhanced sensors and weapons coverage, and facilitating quicker responses to task organization/mission reassignments with enhanced tactical data links that broadcast these command instructions. Options 1, 3, and 4 contribute to minimal organizational impacts. Option 2 would incur problems of

organization primarily due to coalition nations having only Fn Level 0 while the US forces are at Fn Level 3. The US would have difficulty in establishing organizational relationships, mission reassignments, and sensor/weapons pairings due to integration of forces without FORCEnet capabilities.

12.3 Training

It is critical that the Coalition ESG, once formed, operate as a cohesive organization. Under a FORCEnet construct, the utilization of similar communications, data message formats, engagement algorithms, decision aids,…etc. will require that all joint and allied nations participating in a US Navy FORCEnet ensure that appropriate training is developed for personnel. Trained personnel will then operate the various network-centric nodes to ensure readily available assets from sensor, C2, and weapons nodes. Identifying key users from operators to the senior leadership to develop tailored training and educational courses must be done to enhance their network-centric operations knowledge base. Given the software intensive systems that would reside in FORCEnet nodes, simulations and embedded training aids could be heavily relied upon by FORCEnet platforms to sustain skills within the organization. Training could also be extended to multiple platforms based on available communications. A major revision in the logistics curriculum will have to account for provisioning and sparing of COTS and advanced network communications. More operators and maintainers will have to be trained on and be prepared to tackle the issue associated with network maintenance.

12.4 Materiel

Materiel solutions will have to be conceived from a system-of-systems approach. A realigning of coupled legacy system developments/upgrades and newer network-centric technologies must evolve the necessary FORCEnet architecture to include allied nations. Common materiel solutions across the allied platforms must be pursued to maximize interoperability and potential cost reductions.

12.5 Leadership

Commanders and personnel in various leadership roles must understand the need for making decisions in a collaborative environment. Leaders must be aware of all aspects of their FORCEnet platforms (capabilities and limitations) such as to understand their new role in the decision making loop. C2 nodes with improved automated decision aids will relieve commanders and leaders of human in the loop requirements. Sensors that are further reaching will cause leaders to focus beyond what used to be a smaller area of operations/influence on maritime warfare environment. With more dependence on the integration of allied nations, joint and national assets into established coalitions, leaders must have an expanded knowledge base of broader force capabilities and how to employ them. This expanded role of leadership requirements in a FORCEnet construct will incur greater demands in leadership education and training.

12.6 Personnel

It is anticipated there will be no increase in manpower requirements under a FORCEnet construct; however, given the anticipated reduction in personnel and utilization of technically advanced systems, this may pose greater burdens of responsibilities on the users. The development of FORCEnet systems must emphasize a good Human Systems Integration approach to ensure the appropriate workloads are allocated to the user and the systems. The complexities associated with increased data flow and management in a FORCEnet environment will have to be taken into careful consideration as it pertains to human processing capacities. The results of these studies have to be noted early in the development phase such as to make the applicable adjustments to training and doctrine.

12.7 Facilities

FORCEnet applied to shipboard platforms will maximize use of existing stations to perform automated operations that were previously done manually. It is not

anticipated that space requirements will have to be changed to accommodate the FORCEnet architecture implementation for Coalition platforms. It is anticipated that there will be major modifications to links to meet the new network-centric communications interfaces. Shipboard facility requirements will also have to be concerned with providing the increased and uninterruptible power demands for the various FORCEnet C2, Sensor, and Weapons nodes.

Ashore, it is anticipated there will be new or modified facilities to meet the expected demands of FORCEnet lab requirements. Given a system-of-systems approach to achieve the FORCEnet architecture, it is anticipated that there will be heavy utilization of test and lab facilities to ensure equipment operability and connectivity before installing on ships. It is anticipated these facilities will need to be supported during the Operations and Support phase such as to meet continued testing based on changing requirements and tech refresh of hardware. These facilities can also be used by maintenance personnel for troubleshooting as necessary. There should be no increases in existing naval logistics facilities as we anticipate reduced spares storage along with troubleshooting activities that can be performed remotely via networked communications to the FORCEnet equipped coalition platforms.

13.0 Modeling

13.1 Goal

The simulation of the FORCEnet model serves to provide more insight into the network-centric warfare architecture benefits for the Coalition forces. Fully-networked FORCEnet integrates Coalition ships, sensors, networks, command and control, platforms and weapons into a distributive networked combat system, scalable across the spectrum of conflict. The advantage of FORCEnet simulation is that it allows designers to incorporate intricate details with specific requirements based on real information. Simulation also allows designers to obtain simulated results and data in order to compare which FORCEnet level provides the most cost-effective solution to the Coalition forces.

Simulation is relatively easy to apply in theory and can maintain control on experiments such as time.

As described in Section 6, this analysis will focus on the modeling of FORCEnet options for three primary vignettes selected by TTCP Action Group 6. These vignettes are comprised of vignette 3 (Littoral ASuW against the Surface Action Group threat), vignette 6 (Amphibious offload, to put the forces ashore to back up the RP troops against the insurgents), and vignette 7 (Naval Fires support). Although our group did not model all eight vignettes as described in the "Operation Philippine Comfort" Scenario, we performed some initial analysis of the remaining vignettes to set the stage for future modeling by other NPS Cohort groups. This information is contained in Appendix C "Preliminary Modeling Analysis for Vignettes 1, 2, 4, 5, and 8".

13.2 Modeling Tool

ARENA Simulation modeling tool combines the ease of use found in high-level simulators with the flexibility of simulation languages and general-purpose procedural languages such as Microsoft Visual Basic and C-Programming. ARENA simulation modeling is extremely flexible by being fully hierarchical and working up from low-level modules to higher-level modules. Basic ARENA simulation model building blocks are called flowchart and data modules.[23]

Flowchart modules explain the dynamic processes in the model and are typically connected to each other in some way. These flowchart modules function as nodes, places that facilitate flow of entities, origination of flow of entities, and termination of flow of entities. Such flowchart modules include 'Create', 'Dispose', 'Process', 'Decide', 'Batch, 'Separate', 'Assign', and 'Record'.

Data Modules explain the characteristics of various process elements such as entities, resources, and queues. Data modules can setup variables and other types of numerical values and expressions that are tied to the simulation model. Such Data

[23] Model description from Kelton, D., R.R. Sadowski, and D. T. Sturrock, *Simulation with Arena*.

modules include ‘Entity’, ‘Queue’, ‘Resource’, ‘Variable’, ‘Schedule’, and ‘Set’ entities which do not flow through the data modules.

13.3 Description

FORCEnet Levels

For FORCEnet Level 0, voice radio and legacy communication links are used to obtain COP and relay maneuver instructions. FORCEnet Level 1 displays filtered and delayed communication characteristics in order to update and maintain COP. FORCEnet Level 2 offers real-time target information to US and coalition forces. FORCEnet Level 3 allows networked weapon systems to be controlled by national authority level (Note: this particular FORCEnet level was not required as part of the analysis as described in the modeling options of the analysis scenario). FORCEnet Level 4 illustrates fully-networked system for all coalition forces.

Analysis Options

As described in Section 6, five different Coalition FORCEnet ESG options are identified for modeling with ARENA. Option 1 consists of FORCEnet Level 3 US forces with no assistance from the Coalition forces. Option 2 consists of FORCEnet Level 3 US forces with FORCEnet Level 0 Coalition forces. Option 3a consists of FORCEnet Level 3 US forces with FORCEnet Level 1 Coalition forces. The improvement over Option 2 is that the data latency is a significant improvement over the operator delay in the order of magnitudes of time. Option 3b consists of FORCEnet Level 3 US forces with FORCEnet Level 2 Coalition forces. Option 4 consists of FORCEnet Level 4 US and Coalition forces.

Modeled Vignettes

Vignette 3: The objective for vignette 3 was to ensure that SAG was within the ESG's sensing range, to keep SAG in constant surveillance, maintain up-to-date COP and employ efficient allocation of ESG assets for monitoring duty. One assumption made was that a helicopter would add to the ESG's sensing range but would not be able to operate continuously. The minimum COP range was 10nm. The maximum COP range that radar sensors could maintain was up to 50nm. It was assumed that the enemy SAG units would maneuver in a random direction to try to get to the Sulu Sea and not display hostile directions against the ESG units. Coalition High Value Units were assumed to be clustered together and protected by Coalition Ships. Another assumption was that if one or more of the SAG vessels had gone outside of ESG's sensing range, then the entire SAG would go outside the sensing range. For FORCEnet level 2 and higher, Coalition forces would have an enhanced capability in yielding faster data latency in obtaining and sharing target information. For Options 3a & b and higher, Coalition ESG units would all react comparably fast and be ready to act once SAG units began to maneuver. Under Option 2, US forces would be just as effective as Option 3 & 4 and Coalition forces would react once data latency had been reached in obtaining target information. If one of the SAG units maneuvered outside the COP coverage by the ESG Coalition units, then it

would be considered a lost track which means that the monitoring mission performed by the Coalition ESG forces would also be ineffective. In order to counter the movements made by the SAG units, the effectiveness of the Coalition ESG forces relied on the data latency in obtaining and sharing battlefield tactical target information. Level 1 FORCEnet would put out a finite delay time in obtaining and sharing target information among the Coalition forces. The delay time would be large enough to allow SAG units to move out of the COP coverage by the ESG Coalition forces and interrupt the SAG surveillance and monitoring mission. A graphic representation of vignette 3 is listed in Figure 4. Vignette 3 Arena modeling input parameters and processes are listed in Table 3. Figures 5 and 6 shows snapshots of Vignette 3 during a model run (initial positions to T+2 execution)

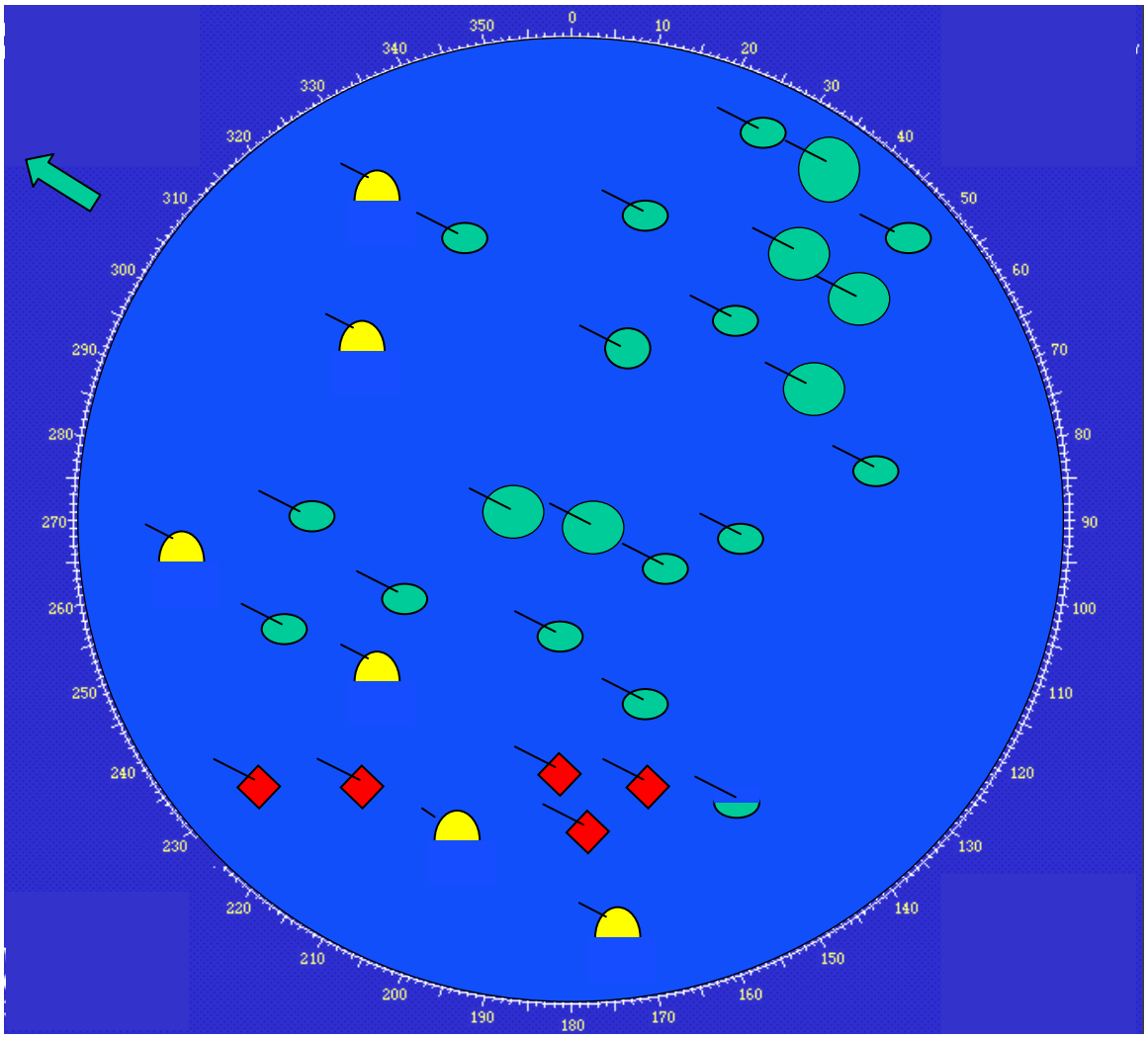


Figure 4. Notional Vignette 3 Operational Formation

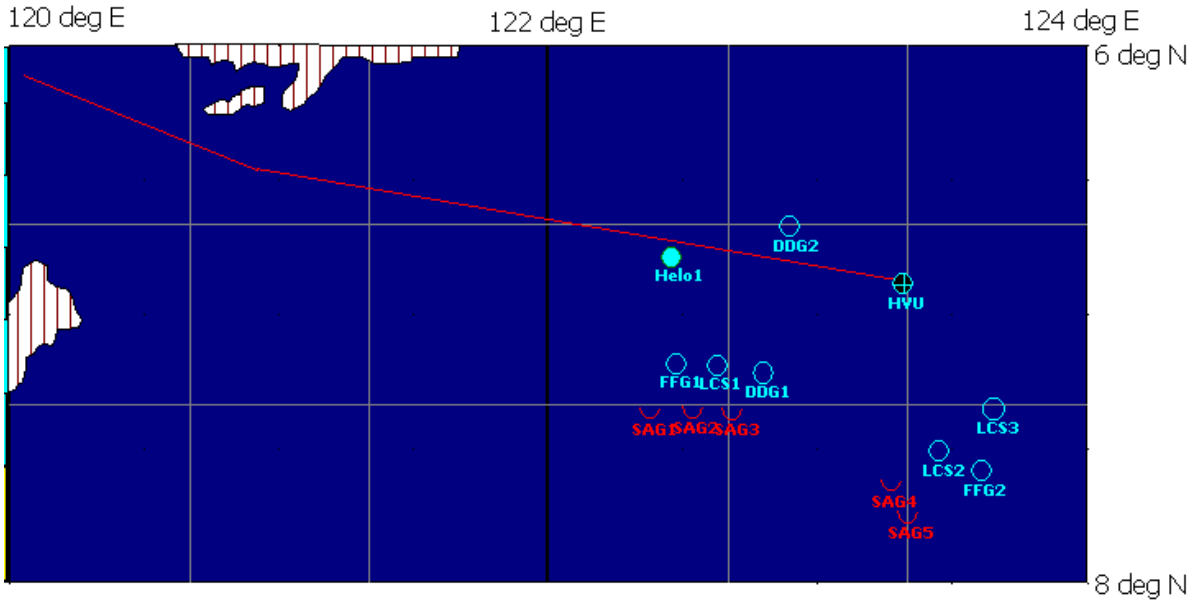


Figure 5 - Vignette 3 Screenshot of Initial Ships' Positions

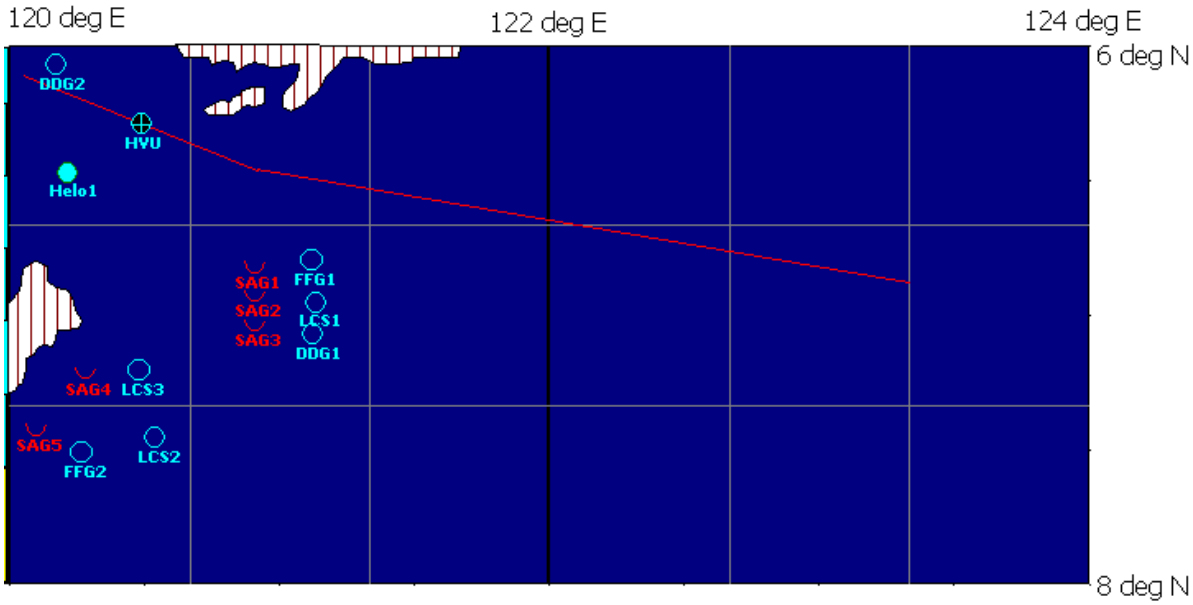


Figure 6 - Vignette 3 Screenshot of Ships' Positions at Time T0 + 2 Days

Process	Fn Level 0	Fn Level 1	Fn Level 2	Fn Level 3	Fn Level 4
Time to trans data from radar sensor to ship's internal network	T(0.02,0.11,0.25)	T(0.02,0.11,0.25)	T(0.02,0.11,0.25)	T(0.02,0.11,0.25)	T(0.02,0.11,0.25)
Time to encrypt the data	T(0.11,0.55,1.21)	T(0.11,0.55,1.21)	T(0.11,0.55,1.21)	T(0.11,0.55,1.21)	T(0.11,0.55,1.21)
Time to transmit data by voice (applicable to level 0 & 1 only)	T(3.98,19.89,43.76)	T(3.62,18.1,39.82)	0	0	0
Time to trans. Data to FORCEnet node (not applicable for level 0)	0	0	T(0.09,0.47,0.96)	T(0.08,0.42,0.93)	T(0.07,0.38,0.83)
Time to decrypt	T(0.01,0.07,0.14)	T(0.01,0.07,0.14)	T(0.02,0.11,0.23)	T(0.02,0.11,0.23)	T(0.02,0.11,0.23)
Time for ship commander to issue instructions	T(4,19.94,43.87)	T(4,19.94,43.87)	T(4,19.94,43.87)	T(4,19.94,43.87)	T(4,19.94,43.87)
Mechanical response time (i.e time it takes for ship to accelerate or change heading)	T(7.1,35.3,77.6)	T(7.1,35.3,77.6)	T(7.1,35.3,77.6)	T(7.1,35.3,77.6)	T(7.1,35.3,77.6)

T – Triangular Distribution

Table 3. Vignette 3 Modeling Input Parameters and Processes

Vignette 6: The objective for vignette 6 was to minimize the time to complete amphibious offload, and ensure effective coverage using ISR assets before and during offload to monitor sea and land threats. One assumption was that land insurgent elements were expected to prevent/attack the offload. Once the Deployment order had been issued, the instruction for coordinating surveillance was issued. Another assumption was that the

US forces would have initial intelligence and ISR information. When the COP was reported, the ready to deploy decision to the beach was granted only if overall COP was complete. Higher FORCEnet levels facilitated the lead time in obtaining complete COP information. During deployment, COP information was also collected. After the COP was reported, instruction to send scouts for reporting was issued. While setting up beach perimeter, instructions would be generated to reposition troops if scouts come back with the report decision. If additional supplies were needed, a request was made. If there was an urgent situation, the beach commander would notify the command and standby. When the beach commander received further orders, intelligence, and COP information, the beach commander would follow instructions and report back the information. A graphic representation of vignette 6 is listed in Figure 7. Vignette 6 Arena modeling input parameters and processes are list in Table 4.

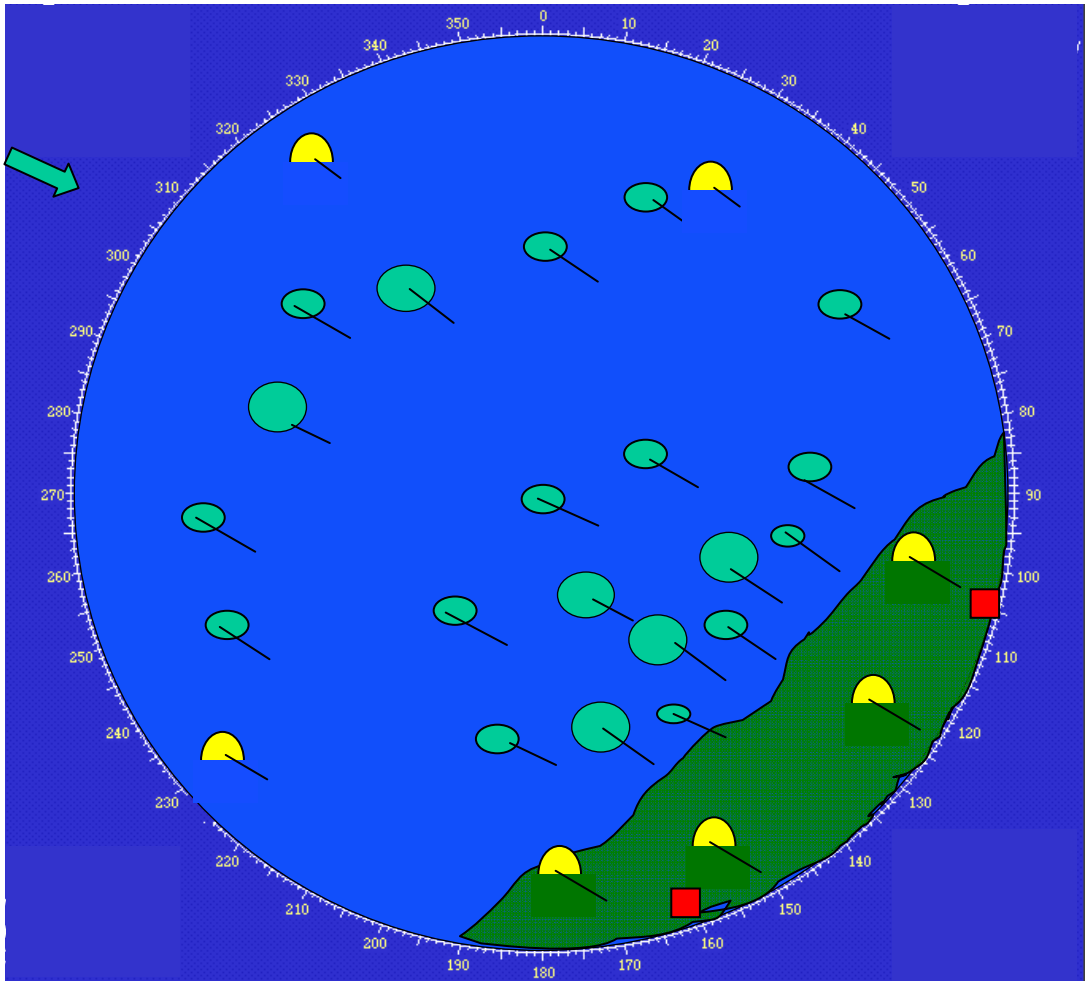


Figure 7. Notional Vignette 6 Operational Formation

Process	Option I		Option II		Option IIIA		Option IIIB		Option IV
Coordinate Surveillance	T(.5, 1, 1.5)		T(.5, 1, 1.5)		T(.5, 1, 1.5)		T(.5, 1, 1.5)		T(.5, 1, 1.5)
Deploy Marines to Beach	T(.5, 3, 4.5)		T(.5, 3, 4.5)		T(.5, 3, 4)		T(.5, 3, 4)		T(.5, 3, 4.5)
Conduct Beach Surveillance	T(.5, 20, 30)		T(.5, 20, 30)		T(.5, 20, 30)		T(.5, 20, 30)		T(.5, 20, 30)
Send Scouts for Report	T(.5, 35, 40)		T(.5, 35, 40)		T(.5, 35, 40)		T(.5, 35, 40)		T(.5, 35, 40)
Setup Beach Perimeter	T(.5, 20, 40)		T(.5, 20, 40)		T(.5, 20, 40)		T(.5, 20, 40)		T(.5, 20, 40)
Reposition Troops	T(.5, 1, 1.5)		T(.5, 1, 1.5)		T(.5, 1, 1.5)		T(.5, 1, 1.5)		T(.5, 1, 1.5)
Call for Additional Supplies	T(.5, 2, 3)		T(.5, 2, 3)		T(.5, 2, 3)		T(.5, 2, 3)		T(.5, 2, 3)

Notify Commander of Situation	T(.5, 10, 15)		T(.5, 10, 15)		T(.5, 10, 15)		T(.5, 10, 15)		T(.5, 10, 15)
Receive Order From Commander	T(.5, 10, 15)		T(.5, 10, 15)		T(.5, 10, 15)		T(.5, 10, 15)		T(.5, 10, 15)
Ready to Deploy Percentage True	50%		50%		66%		75%		90%
Accurate COP Percentage True	50%		50%		66%		75%		90%

T – Triangular Distribution

Table 4. Vignette 6 Modeling Input Parameters and Processes

Vignette 7: The objective of vignette 7 was to effectively suppress truck attacks, destroy any identified truck with rocket launchers, achieve destructive fires after first round or volley, minimize time from Call for Fire to first round impact, and provide timely and accurate BDA of trucks. One assumption was the implementation of Naval Fires Support where naval gunfire support (1 to 9nm) was used with conventional munitions and up to 43nm with Extended Range Munitions. This would be the primary fire engagement means as the need for immediate suppressive fires was also assumed. Another assumption was the immediate execution (Fire When Ready) of fire missions upon weapon systems receiving technical fire control solution (fire mission data) from Naval Fires Control System (NFCS). It was assumed that the enemy threat consisted of 4 hidden trucks with rocket launchers. This means we would have attacks from multiple locations if threat was not destroyed. We could say that if one of the four trucks was not destroyed after the initial counter attack by Coalition forces, it would pop up at another location within 1 mile from original location. Additionally, we assumed the unguided rockets launched from each of these truck vehicles would be up to 4 rockets per truck at about 1 minute intervals (assume a two person crew per truck). It was also assumed that the enemy trucks would be located within a 6nm envelope of the coastal inland region within vicinity of amphibious off load sites. Trucks launching within 4nm would be within 5 inch gun support range and trucks beyond 4nm would be engaged with extended range munitions. It was understood that fewer munitions were required when a more

accurate target location was provided. Another assumption was that long ranging ERGM and/or LRLAP projectiles were available from DDG and CG platforms. It was assumed that enemy locations were identified by our radars upon their initiation of indirect fire; we would respond with immediate indirect fire engagements. It was also assumed that SACC-A, TACC, NFCS and coalition asset equivalents were available for fire support planning/execution. It was understood that Time of Flights would be constant for the scenario as the different Fn Levels were projected to have no impact on time of flight (TOF). It was determined that Ground Marine spotters and UAVs would provide target locations to Naval Surface Fire Support ships. Ground Marine spotters and UAVs provided target detections of trucks launching unguided rockets that inhibited amphibious operations. Given the enhanced camouflage techniques used by the threat, detections were preceded by an observed rocket launch from a specific location. A suppressive fires mission was initiated in a Call for Fire (CFF) format once rocket launch was observed. Next, the CFF was sent to the SACC-A for naval fires support processing. A fire order was then sent to US or Coalition NFCS for fires execution (tactical fire control). The NFCS transmitted mission data to the Gun Fire Control System to generate a technical fire solution for engagement. The gun fired the applicable number of salvos with the total time of fire mission execution based on firing of initial salvo to impact of the last salvo. Ground Marine spotters and UAVs provided battle damage assessment feedback after the fire mission was completed.

After the last fire for effect salvo had impacted, the Ground Spotter or UAV had “eyes on” the target and then developed the battle damage assessment based on the target area destruction. The Battle Damage Assessment was sent to SACC-A for end of mission processing with target suppressed, neutralized, or destroyed. A graphic representation of vignette 7 is listed in Figure 8. Vignette 7 Arena modeling input parameters and processes are list in Table 5.

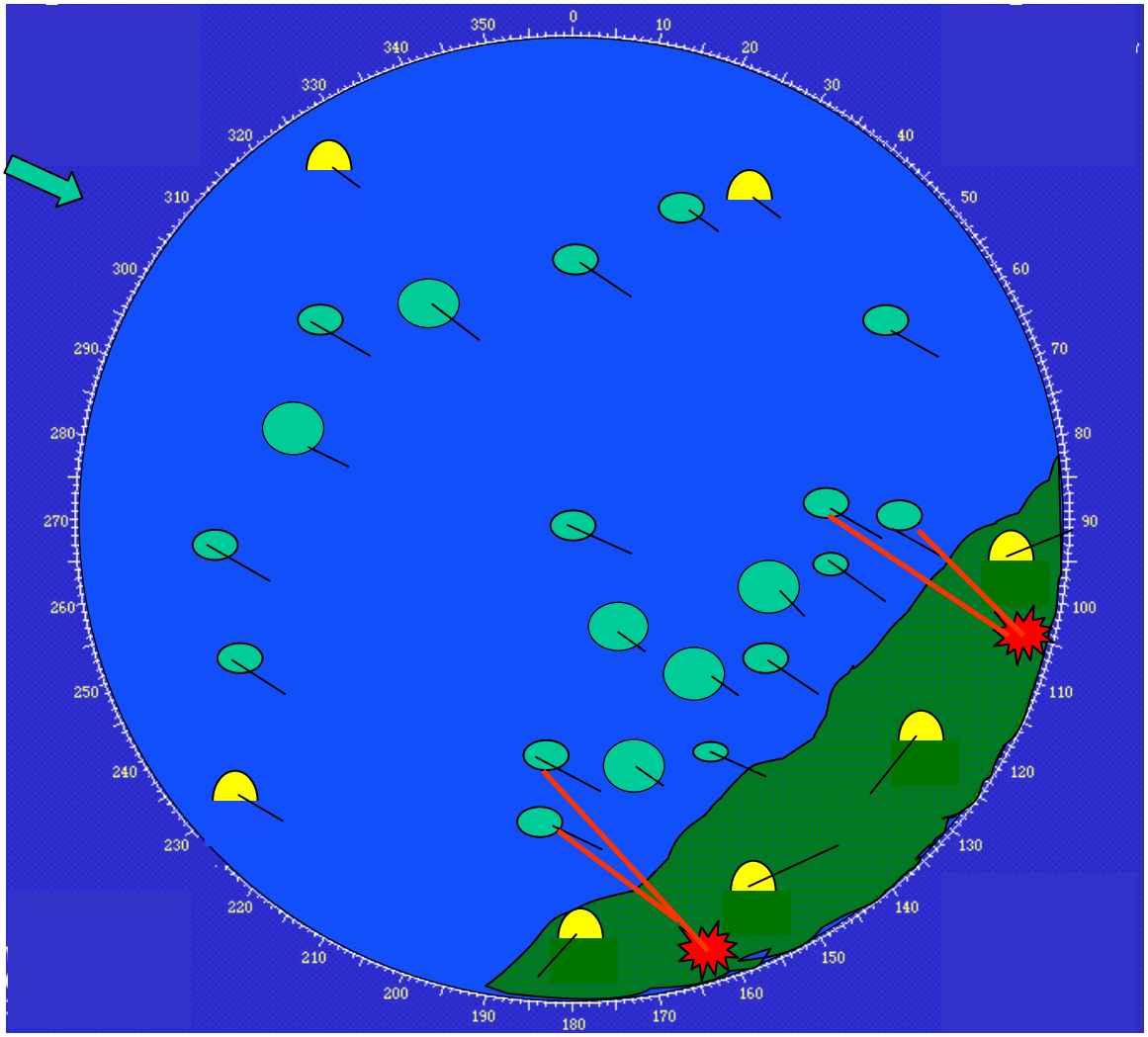


Figure 8. Notional Vignette 7 Operational Formation

Process	Option I		Option II		Option IIIA		Option IIIB		Option IV
Marine Spotter	T(20,40,60)		T(28,48,68)		T(22,42,62)		T(18,38,58)		T(16,36,56)
UAV Spotter	T(45,60,75)		T(55,65,75)		T(47,62,77)		T(44, 58, 73)		T(41,56,71)
SACC A	G(1.5,2)		G(2.25,2)		G(1.75,2)		G(1.35, 2)		G(1.25,2)
DDG/ANZAC	T(50,60,70)		T(55,65,75)		T(52,62,72)		T(48, 58, 68)		T(45,55,65)
CG/AWD	T(50,60,70)		T(55,65,75)		T(52,62,72)		T(48, 58, 68)		T(45,55,65)
GUN FCS	G(1, 2)		G(1.5, 2)		G(1.25, 2)		G(1, 2)		G(0.95, 2)
Fire Target 1	U(32,37)		No Change		No Change		No Change		No Change
Fire Target 2	U(70,75)		No Change		No Change		No Change		No Change
Fire Target 3	U(34,39)		No Change		No Change		No Change		No Change
Fire Target 4	U(32,37)		No Change		No Change		No Change		No Change
Initial BDA	T(10,16,20)		T(14,20,24)		T(12,18,22)		T(8.5,15,18.5)		T(7,13,17)

BDA Truck1	T(10,18,30)		T(14,22,34)		T(12,20,32)		T(8,16,28)		T(6,14,26)
BDA Truck2	T(15,22,30)		T(19,26,34)		T(17,24,32)		T(13,20,28)		T(11,18,26)
BDA Truck3	T(10,18,30)		T(14,22,34)		T(12,20,32)		T(8,16,28)		T(6,14,26)
BDA Truck4	T(10,18,30)		T(14,22,34)		T(12,20,32)		T(8,16,28)		T(6,14,26)
Assign Impact Distance_1	T(1.5,8,10)		T(3,9,12)		T(3,8.5,11)		T(1.25, 7, 9)		T(1,7,9)
Assign Impact Distance_2	T(3,10,11)		T(3,11,15)		T(3,11,13)		T(2.25,8,9.5)		T(2,8,9)
Assign Impact Distance_3	T(1.5,8,10)		T(3,9,12)		T(3,8.5,11)		T(1.25, 7, 9)		T(1,7,9)
Assign Impact Distance_4	T(1.5,8,10)		T(3,9,12)		T(3,8.5,11)		T(1.25, 7, 9)		T(1,7,9)
Target NOT Neutralized	>8		No Change		No Change		No Change		No Change

T – Triangular Distribution

G – Gamma Distribution

Table 5. Vignette 7 Modeling Input Paramters and Processes

Measures of Performance

Vignette 3. Littoral ASuW against the Surface Action Group (SAG) threat.

The Measures of Performances (**MOPs**) for Vignette 3 are as follows:

- **MOP 3.1 - Amount of time SAG is within sensing range:** (Percentage of time within Blue's sensing range): Measured in terms of campaign success of closely shadowing and tracking the maneuvers of the enemy SAG units.
- **MOP 3.2 - Efficiency of asset allocation for monitoring duty:** Measured the time (average seconds) it takes the ESG to respond to a change of heading by a SAG.
- **MOP 3.3 - Maintain up-to-date COP:** Measured in terms of timeliness (average seconds) for maintaining and developing an accurate Common Operational Picture for reporting the precise location of operational location data for friendly and enemy positions.

Vignette 6 - Amphibious offload, to put the forces ashore to back up the RP troops against the insurgents.

The Measures of Performances (MOPs) for Vignette 6 are as follows:

- **MOP 6.1 - Time to complete amphibious offload:** Measured in terms of time to capability (average hours) in regards to the effective amphibious offload mission and campaign success in terms of effective amphibious offload mission without incurring the loss of coalition forces and assets.

- **MOP 6.2 - Ability to coordinate ISR assets before offload to monitor sea and land threats**: Measured in terms of economy by measuring time (average hours) with regard to obtaining a complete intelligence report before the amphibious offload, in order to achieve a successful mission associated with performing the amphibious offload.

- **MOP 6.3 - Ability to coordinate ISR assets during offload to monitor sea and land threats**: Measured in terms of time (average hours) with regard to coordinating satellite imagery, coordinating aerial assets (both organic and non-organic) in order to receive a coherent intelligence report during the amphibious offload to achieve a successful mission.

- **MOP 6.4 - Maintain up-to-date COP:** Measured in terms of timeliness (average seconds) for maintaining an accurate Common Operational Picture in reporting the precise location of operational location data for friendly and enemy positions.

Vignette 7 - Naval Fires support

The Measures of Performances (MOPs) for Vignette 7 are as follows:

- **MOP 7.1 - Number of rounds taken to suppress truck attack:** Measured in terms of economy of comfort in order to allocate the minimum number of rounds necessary to suppress the enemy truck attacks.
- **MOP 7.2 - Time taken to suppress truck attack :** Measured in terms of time (average seconds) from call for fire initiation followed by weapons systems

engagement until last round of a salvo lands in target area to suppress the enemy truck attacks.

- **MOP 7.3 - Number of trucks destroyed:** Measured in terms of effectiveness of engagement by assessing how many of the four detected trucks were destroyed based on timeliness and proximity of rounds landing at the target.
- **MOP 7.4 - Number of trucks escaped:** Measured in terms of effectiveness of engagement by assessing how many of the four detected trucks escaped based on timeliness and proximity of rounds landing at the target.
- **MOP 7.5 - Accuracy of first round falls of shot:** Measured in terms of accuracy (meters) of first rounds landing at vicinity of reported target location.
- **MOP 7.6 - Time taken from call to fire, to first round impact:** Measured in terms of economy of comfort in regards to the response time from Call for Fire generation of the enemy target to impact of the initial round in the target area (average seconds). The longer the response time, the more likely it is for the enemy target to move away to a different location.
- **MOP 7.7 - Time taken from first anti-coalition attack to BDA confirming target neutralized**: Measured in terms of time to capability (average seconds) in regards to the confirmation that the target has been destroyed.

13.4 Results

After definition of the various vignette process blocks in Arena with applicable distributions assigned to process parameters, we ran the simulations for each vignette and generated the Arena output data captured in the Table 6 for each of the vignettes.

13.4.1 MOP Results

Based on output from Arena as reflected in Table 6, it appears that Option IV with the Coalition platforms configured with FORCEnet Level 4 performed best in all of the analyzed events. Some of the more notable differences based on review of the table

include MOP's 3.4 and 6.4 "Maintain up-to-date COP". Although Options 1 (US FORCEnet Level 3), 3b (Coalition FORCEnet Level 2), and 4 (Coalition FORCEnet Level 4) were very close, the results for FORCEnet Level 4 did stand out as providing the best COP for all vignette. There was definitely a noticeable difference in the COP updates for Option 2 (Coalition FORCEnet Level 0) and Option 3a (Coalition FORCEnet Level 1) ranging at update rates from 18 to 28 seconds as compared to Option 4 (Coalition FORCEnet Level 4) at from .79 to 3.4 seconds. For vignette 6, it seems Option 1 (US FORCEnet Level 3) had a better COP update outcome than for Option 4 (Coalition FORCEnet Level 4). This could be due to the configuration of a more cohesive, all US forces ESG than an expanded Coalition ESG with more platforms to consider in the COP update. One of the major performance drivers for FORCEnet is the ability to capture a timely situational awareness picture. Particularly, in a fluid operational scenario during which platforms are maneuvering, the timely updates provided by FORCEnet Level 4 would also directly correlate with a more accurate picture of the platform locations.

In most cases, the modeling performance results showed that Options 1, 3b, and 4 were fairly close in MOP results except for MOPs 6.1, 6.2, 6.3, and 7.7. Basically, for MOPs 6.1, 6.2, and 6.3, using FORCEnel Level 4 for the Coalition platforms resulted in half the time it took as compared with FORCEnet Level 2 (Option 3b) to complete amphibious offload and to co-ordinate ISR assets before and during offload. These results could be attributed to process times that had been shortened due to established Resource Managers that more expediently processed command instructions and sensor assignments. The Resource Managers were able to do this based on enhanced knowledge of C2, sensor, and weapons platform's mission needs, operational status, and data information requirements.

As for vignette 7 results, Option 4 outperformed all other options after reviewing the MOP results; however, Option 1 and 3b did perform equally well when it came to the number of trucks destroyed and the number of trucks escaped. The performance difference between Option 4 (Coalition FORCEnet Level 4) and Option 3b (Coalition

FORCEnet Level 2) is so close that another discriminator such as cost analysis would have to be considered as part of a sensitivity analysis (see Section 14).

13.4.2 MOE RESULTS

Based of the specific vignettes selected for analysis (3, 6, and 7), the MOE's that were more applicable for getting good assessments based on the selected MOP's were MOE 1 "Time to Capability" and MOE 4 "Campaign Success". Vignette 3 MOP's strongly contributed to getting good "Campaign Success" results for Coalition FORCEnet 4. For vignette 6, Coalition FORCEnet Level 4 also contributed to an enhanced performance in MOE 1 "Time to Capability" and MOE 4 "Campaign Success" through achieving the best MOP measurements for MOP's 6.1, 6.2, and 6.3.

As for MOE 2 "Economy of Effort", the performance results for MOP 3.2, MOP 6.2, MOP 6.3, and MOP's 7.1 thru 7.4 showed that Option 4 (Coalition FORCEnet Level 4) would significantly contribute to a better effectiveness for economy of effort. Although, option 1 (US FORCEnet Level 3) and 3b (Coalition FORCEnet Level1 2) did equally as well with MOP 7.3 and 7.4, Coalition FORCEnet Level 4 did produce results that indicated a noteworthy improvement in economy of effort for the Coalition ESG.

As for MOE 3 "Risk", the only vignette that best contributed to making an assessment in this area was vignette 3 with MOP 3.2 "Keep SAG in constant surveillance". For this MOP, both options 3b and 4 had the best results such as to minimize the risk in Coalition ESG operations. However, it is the cost analysis in the next section that will determine what is most cost effective for the coalitions given that the MOP outcomes for Coalition FORCEnet Level 2 and 4 come out with nearly the same results.

Table 6. Arena Output for Modeled Vignettes

Vignette	MOP	Description	Option I	Option II	Option IIIA	Option IIIB	Option IV	Most Effective Option for MOP
Vignette 3. ASuW against the SAG threat	3.1	*Amount of time SAG within sensing range. (Percentage)*	97.8	97.1	97.3	97.2	98.1	Option IV
	3.2	*Keep SAG in constant surveillance (Average Seconds)*	55.963	68.172	66.471	53.358	53.139	Option IV
	3.4	*Maintain up-to-date COP (Average Seconds)*	0.843	18.34	16.78	0.863	0.794	Option IV
Vignette 6. Amphibious Offload	6.1	*Time to complete amphibious offload (Average Hours)*	4.61	5.12	4.4	3.87	1.89	Option IV
	6.2	*Ability to co-ordinate ISR assets before offload to monitor sea and land threats (Average Hours)*	1.51	1.89	1.48	1.24	0.54	Option IV
	6.3	*Ability to co-ordinate ISR assets during offload to monitor sea and land threats (Average Hours)*	0.29	0.6	0.422	0.218	0.141	Option IV
	6.4	*Maintain up-to-date COP (Average Seconds)*	2.16	28.8	24.84	5.04	3.42	Option I
Vignette 7. Naval Fires support	7.1	*Number of rounds taken to suppress truck attack (Average Number of Rounds)*	5.37	6.23	6.1	5.06	4.42	Option IV
	7.2	*Time taken to suppress truck attack (Average seconds)*	394.66	426.22	421.99	338.53	324.17	Option IV
	7.3	*Number of trucks destroyed (Average Number of Trucks)*	4	2	3	4	4	Option I, IIIB, & IV
	7.4	*Number of trucks escaped (Average Number of Trucks)*	0	2	1	0	0	Option I, IIIB, & IV
	7.5	*Accuracy of first round falls of shot (Average meters)*	6.55	7.53	7.58	6.27	5.84	Option IV
	7.6	*Time taken from call to fire, to first round impact (Average seconds)*	101.06	110.45	105.59	98.71	94.61	Option IV
	7.7	*Time taken from first anti-coalition attack to BDA confirming target neutralized (Average seconds)*	197.71	233.94	195.4	199.85	175.39	Option IV

13.5 Limitations

Due to the complexity of the project, an extensive amount of time was required to conduct trade studies and implementation of the modeling. A number of assumptions were made based on the performances of existing systems and current naval doctrines. In addition, verification and validation are difficult to prove due to the lack of obtainable data.

13.6 Modeling Conclusions

Option 4 (Coalition FORCEnet Level 4) is recommended as the implementation for the Coalition forces based on the Arena modeling results. Further cost analysis that compares Coalition FORCEnet Levels 4 and 2 will be needed to determine the overall best solution. Given the close performance of Options 3b and 4 obtained from the Arena modeling results, this cost analysis will be needed as critical part of our overall analysis for the sake of proposing a recommendation between FORCEnet Levels 2 and 4.

14.0 Program Affordability

This section provides the economic analysis and guidance based on a Cost Estimation Model reflecting a capability-phased approach. The phases are developed and acquired using spiral development. Furthermore, the model serves as a tool to gain insight into the requirements to develop, acquire, and support the different levels of capability. Consideration is given to total system life cycle costs required to integrate network-centric technology into allied fleets. The rationale for spiral acquisition is that it allows for the program to aggregate incremental capabilities more quickly, thus giving the coalition greater capabilities sooner with the inherent mechanism accommodating lessons learned and patch insertion. Another advantage of a spiral acquisition is that risks can be spread across a series of spirals, with the added benefit of allowing the user to develop tactics, techniques, and procedures incrementally as well. Each spiral acquisition

can seamlessly respond to lessons learned from preceding spirals. Technology improvements can be incorporated into the fleet faster—lean, agile acquisition by its very nature. Lastly, the main advantage is that the US would incur the bulk of the research and development cost by leveraging off of existing proven technologies; thus giving the Coalition forces an incentive to integrate the proven FORCEnet technology into their fleet at a lower cost.

14.1 Overview

The options and capability provisions of each option are described in detail in Section 6 and were developed in accordance with the Statement of Work, gap analysis results (Initial Capabilities Document) and program strategy (Section 5). The options or FORCEnet levels of capability are applied to situational levels provided in the TTCP and were simulated accordingly as described in Section 13. All of these are considerations and inputs to the economic analysis developed using the methodology found in the report titled "Cost Considerations in Systems Analysis" by Gene Fisher.[24] In summary, the goal of the analysis is to provide a relationship between the cost and capability with the following assumptions set forth.

The default baseline technology level for Coalition FORCEnet capabilities sets the US force at FORCEnet Level III and all Coalition forces at FORCEnet Level 0. Within the context of developing Coalition FORCEnet Economic Cost Model, the scope is limited to costing FORCEnet Option 3A (US force with FORCEnet Level I & Coalition forces with FORCEnet Level I or II), Option 3B (US force with FORCEnet Level II, and Option 4 (US force with FORCEnet Level IV & Coalition forces with FORCEnet Level IV) for the Coalition forces.

Table 7 provides a high level view of the integrated cost breakdown associated with acquisition and O&S cost. Important elements towards implementing a successful

[24] Fisher, Gene H., *Cost Considerations in Systems Analysis*, Prepared for Office of the Assistant Secretary of defense (Systems Analysis), American Elsevier Publishing Co., Dec. 1970.

Coalition FORCEnet in the fleet would be to determine the most cost-effective system design to achieve the desired level of FORCEnet integration.

	Acquisition	Operation and Support
Software Build/Procurement	X	
Hardware Procurement	X	
Hardware Installation and Test	X	
Software Test	X	
Installation	X	
Initial Training	X	
Initial Spares	X	
Administrative and Logistics Cost	X	
Civilian Personnel Labor Cost	X	X
System Integration Cost	X	X
Curriculum Development	X	X
Configuration Management	X	X
Replenishment Spares		X
Consumables		X
Test Equipment		X
Ongoing Training		X

Table 7. Estimated LCC for Coalition FORCEnet

14.2 Assumptions

In order to construct a complete overall system life cycle cost for the FORCEnet integration of the Coalition forces, the following assumptions apply:

- All costs are stated in FY 2006 dollars. (The fiscal year begins in October 1, 2005 and ends in September 30, 2006.)
- Inflation is not considered, thus constant-dollar values (real) are used.
- Interest rate use is real as published in the OMB circular A-94 for cost effectiveness analysis when discounting Life Cycle Costs (LCC) of alternatives.

- Payments are made at the end of each fiscal year.
- Sunk costs are ignored.
- RDT&E is a non-recurring program cost that must be paid prior to acquisition cost of any alternative (if it applies)
- Operation and Support have real cost growth of X % beginning Y years after initial procurement.
- Training is divided into initial (procurement) and annual training following implementation of the option under consideration. The annual training costs consider "just-in-time" training due to attrition or system upgrades or refresh and would show up as the Operation & Support costs.
- Military Construction is not considered
- Salvage value will not be considered in this analysis.
- Integration Costs will be correlated with the complexity of the platform
- Total cost is per unit (platform will be specified)

14.3 Life-Cycle Costs

The intent of this model is to provide an initial cost reflecting acquisition of resources required to attain capabilities using an incremental approach. Although research and development, acquisition, operation and support, and disposal are considered essential to a realistic and comprehensive economic model, consideration has been given to the nature of net-centric warfare, i.e., it is COTS and software driven, thus the bulk of the cost is in the acquisition of the initial capability, and its corresponding and applicable logistic elements. The paragraphs below address each aspect of total life cycle costs and how each one will be treated in this model.

14.4 Research & Development

The Coalition FORCEnet leverages off of previously resourced R&D efforts by adopting current successful technology, integrating and tailoring the design in order to suit the nature of the application. By splitting acquisition process into three separate spirals, it allows engineering activities to implement lessons learned quickly into the next spiral development. In this context, the R&D costs would be perceived as the procurement costs.

14.5 Acquisition

The Coalition FORCEnet acquisition is broken into three separate spirals. The first spiral (FY2006-2009) would focus first on the command and control capabilities through a CENTRIXS like capability. The second spiral (FY2010-2014) would implement a tactical data link enhancement capability, and enhanced communications (IP and Voice Over IP) capability. The third spiral (FY2014-2018) would develop and field a CEC like capability and implement enhanced network connectivity into the weapons systems for command authority engagements. The separate spiral acquisitions allow for enhancement of the processes for using FORCEnet tools and evenly distributed investment dollars for overall desired capabilities rather than a huge initial investment without an immediate payoff. The acquisition costs include the System Procurement Cost, Installation Cost, Initial Training Cost, Initial Spares and Logistics Cost.

In order for a Coalition Partner to achieve a FORCEnet Level I capability, the coalition FORCEnet acquisition would need to take on Spiral 1. In order for a Coalition Partner to achieve a FORCEnet Level II capability, the coalition FORCEnet acquisition would need to take on Spirals 1 and 2. In order for a Coalition Partner to achieve a FORCEnet Level IV, the coalition FORCEnet acquisition would need to take on Spirals 1, 2 and 3.

14.6 Operation and Support

The operation and support required for the different levels of capability is critical towards providing a seamless FORCEnet transition for the coalition partners. The procurement costs only covers the initial technical documentation (operation and maintenance manuals), along with some initial training and its corresponding material. As far as spares are concerned, most equipment is COTS, thus the maintenance philosophy is remove and replace at the highest level.

The coalition partner is advised that due to the three separate spiral acquisition intervals, the operation and support costs during these three periods will fluctuate accordingly. The first spiral focuses on the command and control capabilities the Coalition FORCEnet project would incur lower O&S costs per unit than the second spiral mainly due to the introduction of the upgraded communications and tactical data link during the second phase. The third spiral would incur the most O&S costs out of the three spirals because it receives an expanded capability in network connectivity of the Coalition FORCEnet. For upgrades to FORCEnet Levels II and IV, Coalition partners would incur slightly higher O&S costs because of the embedded integrated costs associated with the transition of existing capabilities to accommodate Spiral II and Spiral III acquisition processes.

14.7 Cost Summary

Spiral #1 (FY2006-2009) Command and Control: CENTRIXS units for each unit within the coalition force (IP based)

Spiral #2 (FY2010-2014) Tactical Data Link: Link 22 capability for each unit within the coalition force (highly enhanced tactical data link) and Communications: JTRS tactical programmable radio system

Spiral #3 (FY2014-2018) CEC-like capability, enhanced networks and connectivity into combat systems, weapons and engineering networks, and communication bandwidth connectivity which include space satellites and shipboard satellite antennas.

When projecting the procurement costs of FORCEnet for coalition partners, it is important to consider the learning curve and initial integration cost factors that would lower the total program costs if multiple ship installations are involved.

When projecting the operation and support costs of FORCEnet for coalition partners, it is important to consider the embedded integration costs factors associated with the transition of existing capabilities to accommodate Spiral II and Spiral III acquisition processes.

Table 8 shows cost to bring Coalition FORCEnet to FORCEnet Level I through Spiral #1 (FY2006-2009) process that provides Command and Control capability: CENTRIXS like capability for each unit within the coalition force (IP based).[25]

Item	**Cost (M)**
System Integration Cost	2.00
Software	0.05
Hardware	0.50
Admin and Logistics Cost	0.10
Installation	0.40
Initial Training	0.01
Initial Spares	0.14
Total	**3.20**

Table 8. FORCEnet Level 1 Cost Estimation Model (in FY2006 $)

Table 9 shows cost to bring Coalition FORCEnet to FORCEnet Level II through Spiral #2 (FY2010-2014) process that provides the Tactical Data Link capability: Link 22 capability for each unit within the coalition force (highly enhanced tactical data links) and Communications: JTRS tactical programmable radio system communications.[26]

[25] Representative costs collected via verbal interviews with PHD CEC engineers. Cost Estimation Model using relevant costs were calculated by applying "Discounted Cost /Present Value calculation method" from NPS course SI3011- Engineering Economics and Cost Estimation.

Item	Cost (M)
System Integration Cost	3.40
Software	0.40
Hardware	0.70
Admin and Logistics Cost	0.20
Installation	1.00
Initial Training	0.05
Initial Spares	0.15
Total	**5.90**

Table 9. FORCEnet Level 2 Cost Estimation Model (in FY2006 $)

Table 10 shows cost to bring Coalition FORCEnet to FORCEnet Level IV through Spiral #3 (FY2014-2018) process that provides CEC-like capability, enhanced networks and connectivity into combat systems, weapons and engineering networks, and communication bandwidth connectivity, including space satellites and shipboard satellite antennas.[27]

Item	Cost (M)
System Integration Cost	9.60
Software	1.00
Hardware	3.30
Admin and Logistics Cost	0.50
Installation	1.60
Initial Training	0.20
Initial Spares	0.60
Total	**16.80**

Table 10. FORCEnet Level 4 Cost Estimation Model (in FY2006 $)

[26] Same cost method as applied for FORCEnet Level 1.

14.8 Costs Estimation Conclusion

Total Cost = R&D Costs + Acquisition Costs + Operation and Support Cost.[28]

Based on spiral methodology, R&D and Acquisition Costs are considered Procurement Cost. Figure 9 provides the profile of the overall LCC for FORCEnet level I, II, and IV.

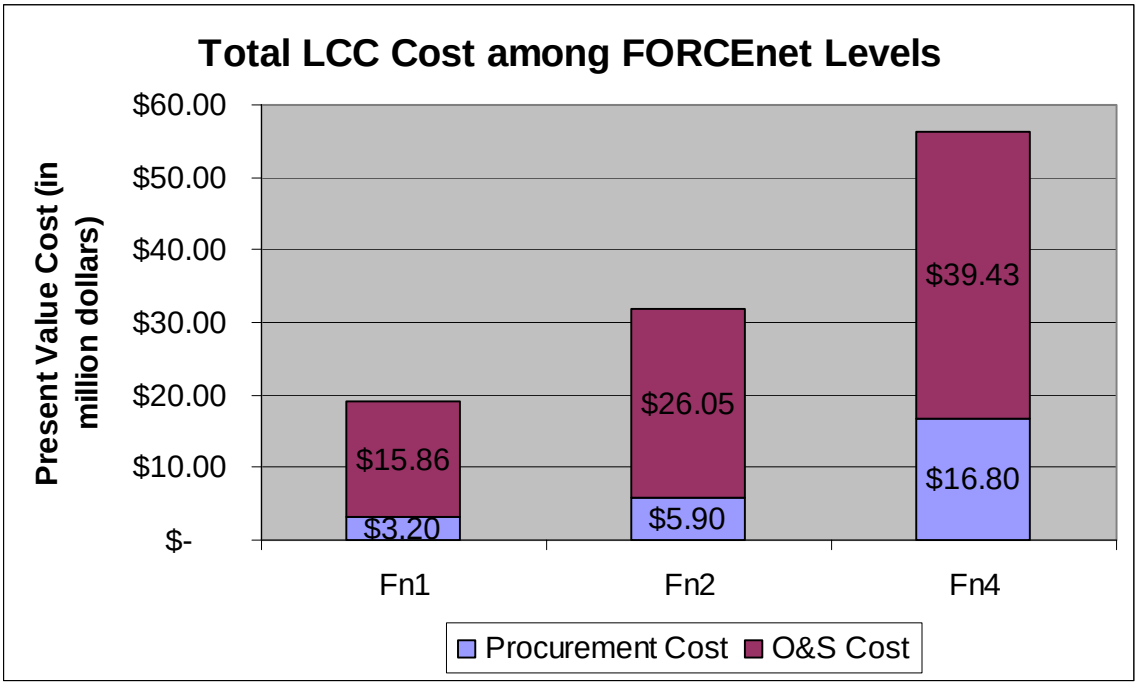


Figure 9: Total Life Cycle Costs for FORCEnet Levels I, II & IV

Procurement costs are most likely fixed costs while O&S costs are more likely fluctuated due to uncertainty of requirements and operational conditions of the system in the later years. The O&S costs exceed the actual costs of procurement, therefore performing the sensitivity cost analysis on O&S costs would be more realistic in terms of predicting the unexpected costs over the life span of the system.

---

[27] Same cost method as applied for FORCEnel Level 1 on previous page.

[28] Typical Life Cycle Cost formula taken from NPS course SI3011Engineering Economics and Cost Estimation

Figure 10 provides the output of the O&S sensitivity cost analysis.[29] The sensitivity analysis evaluates the effect of change in annual O&S costs from 0% to 100% starting in year 11 (2016) due to maintenance costs such as software and hardware upgrades, modifications, and parts replacements. Assuming there will not be R&D costs and the O&S costs will be impacted by changes from 0% to 100% annually starting year 11 (2016) through year 20 (2025), and further based on the calculations and the sensitivity graphs, a robust decision could be made to achieve system effectiveness and cost savings. FORCEnet levels I and II would have less cost increase impact than FORCEnet level IV in the latter years; but of course, they would have fewer capabilities as well. With the fluctuation in overall O&S costs yearly starting at year 11, total O&S costs for Level IV could be over-budgeted by approximately by $27M versus $14.5M for level II and $6.5M for level I. Therefore, the best option is FORCEnet Level II with its best value for the money.

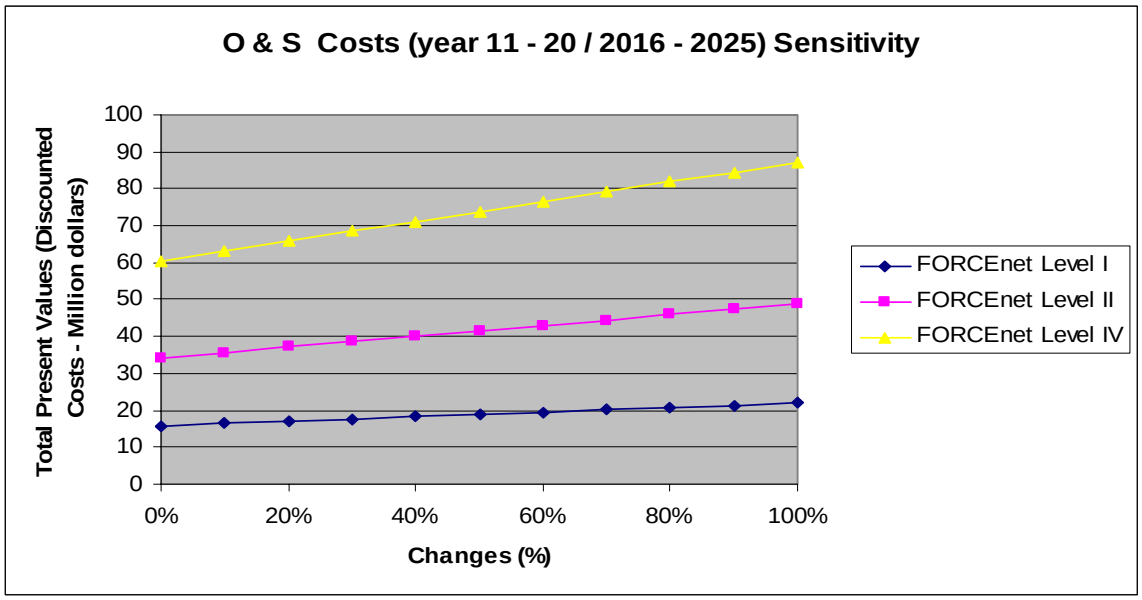


Figure 10: O & S Costs Sensitivity Analysis

[29] Cost Effectiveness Analysis via Sensitivity Analysis was applied to analyze complications with comparing alternatives based on NPS course SI3011- Engineering Economics and Cost Estimation.

15.0 Future Studies and Expectations

15.1 Future Studies

PHD Cohort #4 used Arena software for modeling. The Arena software was provided as a businesses tool to model operational performance. The cohort was able to use the software to provide modeling and simulation of the different phases within the scenario.

Future studies should also take into account other modeling software to ensure a comprehensive analysis has been accomplished. Cohort #4 found another software application, STK (Satellite Tool Kit), for modeling and simulation which could have been used to provide a valuable comparative analysis. However there was not enough time to become familiar with the software.

15.2 Future Expectations

Moving forward through the implementation of FORCEnet and the methods for sharing data within the coalition maritime forces, Cohort #4 discussed many alternatives. Several of these alternatives, while very attractive, were very abstract and unconventional in their methods.

Data classification – Multi –Level Security (MLS) remains a concern within the coalition forces. Data segregation and classification using standard encryption methods and a separate encryption key for each classification method could be replaced using a router based system having the same encryption method, thereby possibly eliminating some of the overhead. The router based system could be based on metadata being attached to the data packets moving across the network. The metadata determines which IP addresses are allowed to receive data and which IP addresses data should be received from. The router could be strictly controlled in a large deck or shore environment with the bandwidth and processor capability to handle the amount of throughput required. [30]

[30] Data classification summarized from “The Formal Representation of Administrative and Operational Relationships within Defense Organizational Constructs”, 2006, Sam Chamberlain, Ph.D.

Data prioritization – The same type of method described above could be used to prioritize data for time sensitive data being passed across the network such as engagement data. For example, if a unit has important traffic to pass such as engagement data, its metadata could now contain a bit that gives it priority across the network, thereby cutting down on the data latency and speeding the communication. [31]

Disposable communications satellites – As time progresses, an ESG may require a disposable communications satellite for emergent operations. The disposable satellite would be sent into low earth orbit and be designed to provide high speed communications in any area of the world just for the purpose of ESG operations in the area. At a predetermined time, the satellite would be allowed to enter the earth's atmosphere and therefore burn-up upon re-entry. The disposable satellite could also provide ISR if so designed. [32]

Distributed agent software/hardware – Having the main agent in one location has advantages of less data conflicts across the network, ease of upgrade and operation. However the distributed function allows for semi-autonomous actions, redundancy and speed of capability.

Load Balancing – Load balancing would inherently reduce the amount of throughput and overhead required by the network. However, significant robust and capable networks would need to be examined and are perceived to be more expensive with regard to the amount of programming required to achieve such a concept. If the amount of software programming were approved, it is anticipated that the speed of operations would be enhanced.

[31] Data prioritization summarized from "Integrating Multilevel Command and Control into a Service Oriented Architecture to Provide Cross Domain Capability", 2006, Christopher John Raney

[32] Signal Magazine, July 2006, Delay Ignites Frustration, By Maryann Lawlor http://www.afcea.org/signal/articles

APPENDIX A: INTEGRATED ARCHITECTURE PRODUCTS

THIS PAGE INTENTIONALLY LEFT BLANK.

A.1 High Level Operational Concept (OV-1)[33]

A.1.1 Product Definition

The High Level Operational View High Level Concept Graphic product (OV-1) is the most general of the architecture description products. It describes a mission and highlights main operational nodes that are unique to operations. The OV-1 provides a description of the interactions between the subject architecture and its environment.

A.1.2 Product Purpose

The purpose of the OV-1 is to provide a quick high-level description of what the architecture is supposed to do and how it is supposed to do it. This product can be used to orient and focus detailed discussions. The main utility of the OV-1 is a facilitator of human communication intended for presentation to high-level decision makers.

A.1.3 Product Overview

In figure A.1.1, the Coalition Expeditionary Strike Group (CESG) Operational View Concept Graphic depicts a general sample of the notional architecture for future use by the coalition. Figures A.1.2 through A.1.4 show the OV-1 diagrams defined for each of the scenario vignettes for analysis. The architecture depicts the general flow of information from the Joint FORCEnet links to the Coalition platforms of the ESG where the data is used to support tactical and intelligence needs. The interfaces shown between ships support mainly message traffic that is necessary to coordinate intelligence and targeting activities. There are other interfaces reflected to show external linkages to joint and national assets.

[33] Diagram type descriptions to follow from DOD Architecture Framework Version 1, 9 Feb 2004, “Definitions and Guidelines”

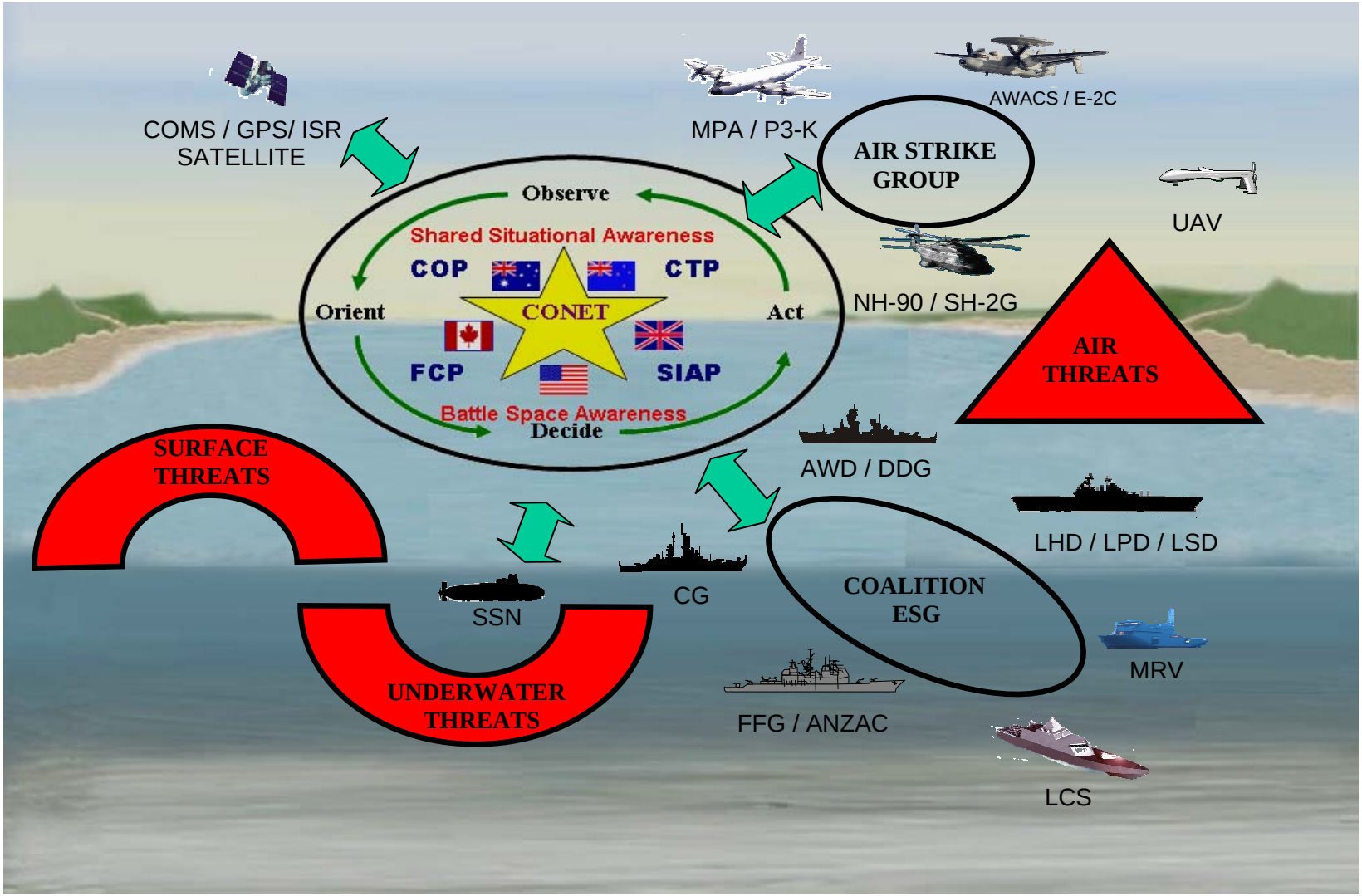


Figure A.1.1. Overall Coalition FORCEnet OV-1

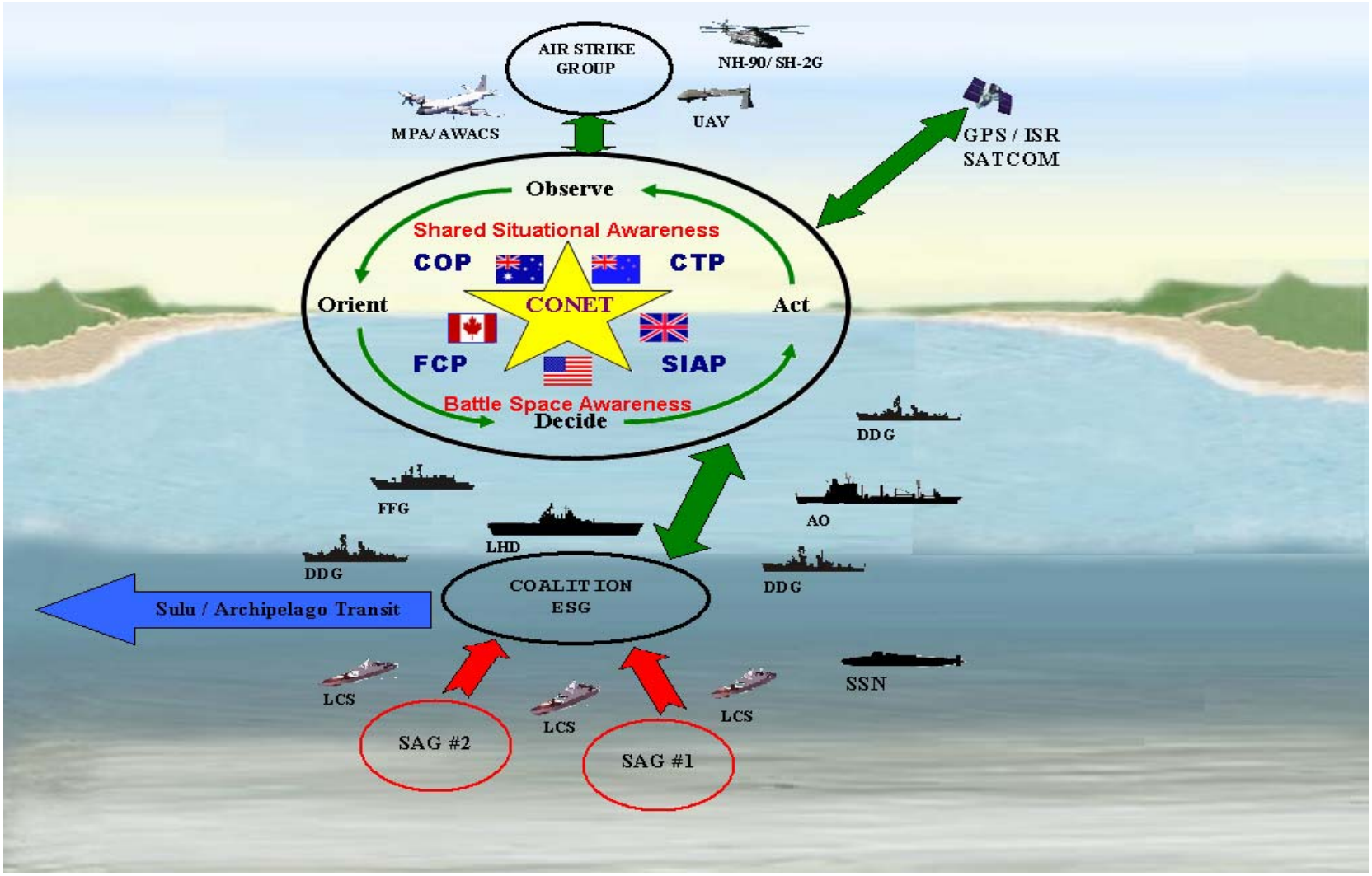


Figure A.1.2. OV-1 for Vignette 3: ASUW Against the SAG Threat

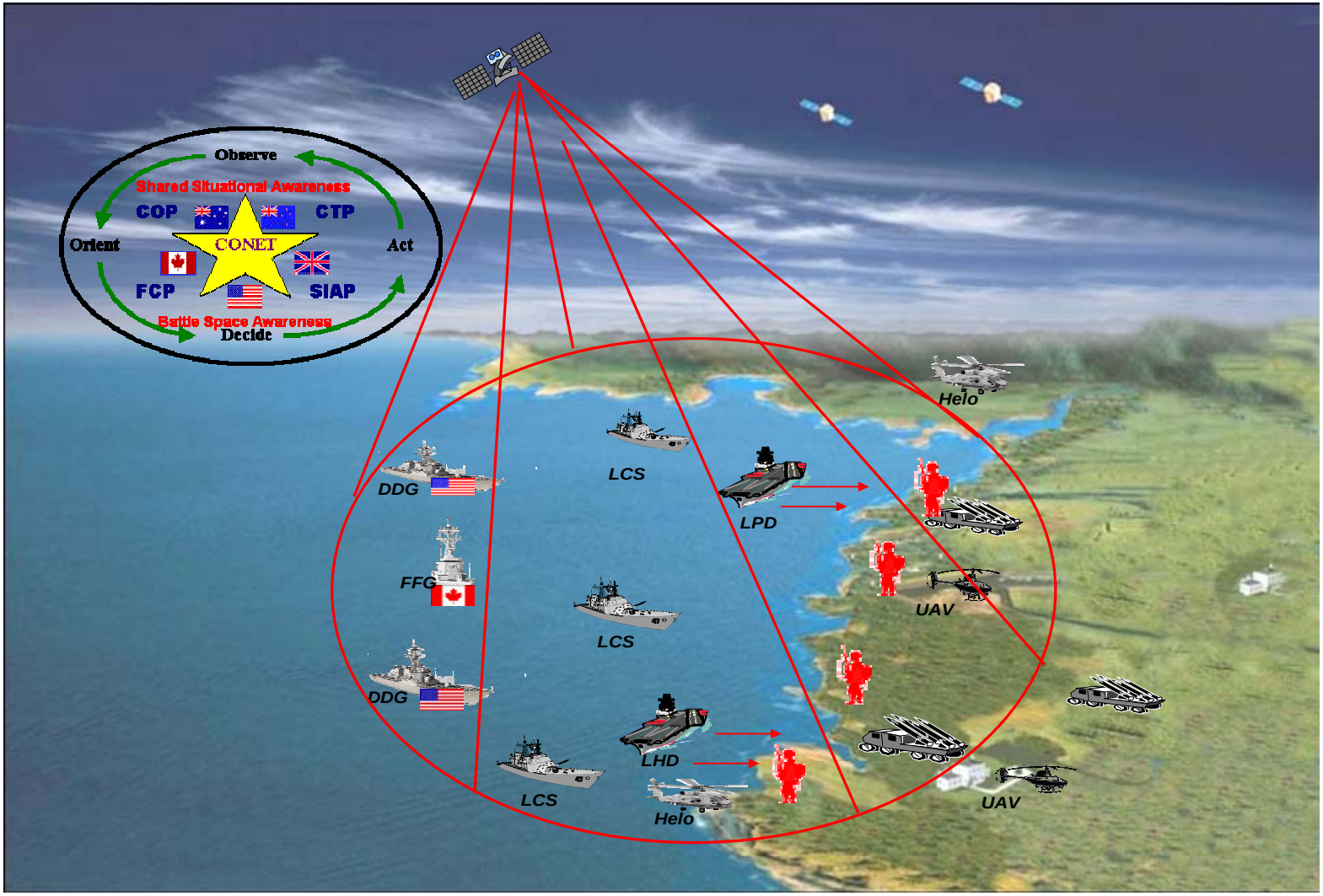


Figure A.1.3. OV-1 for Vignette 6: Amphibious Offload

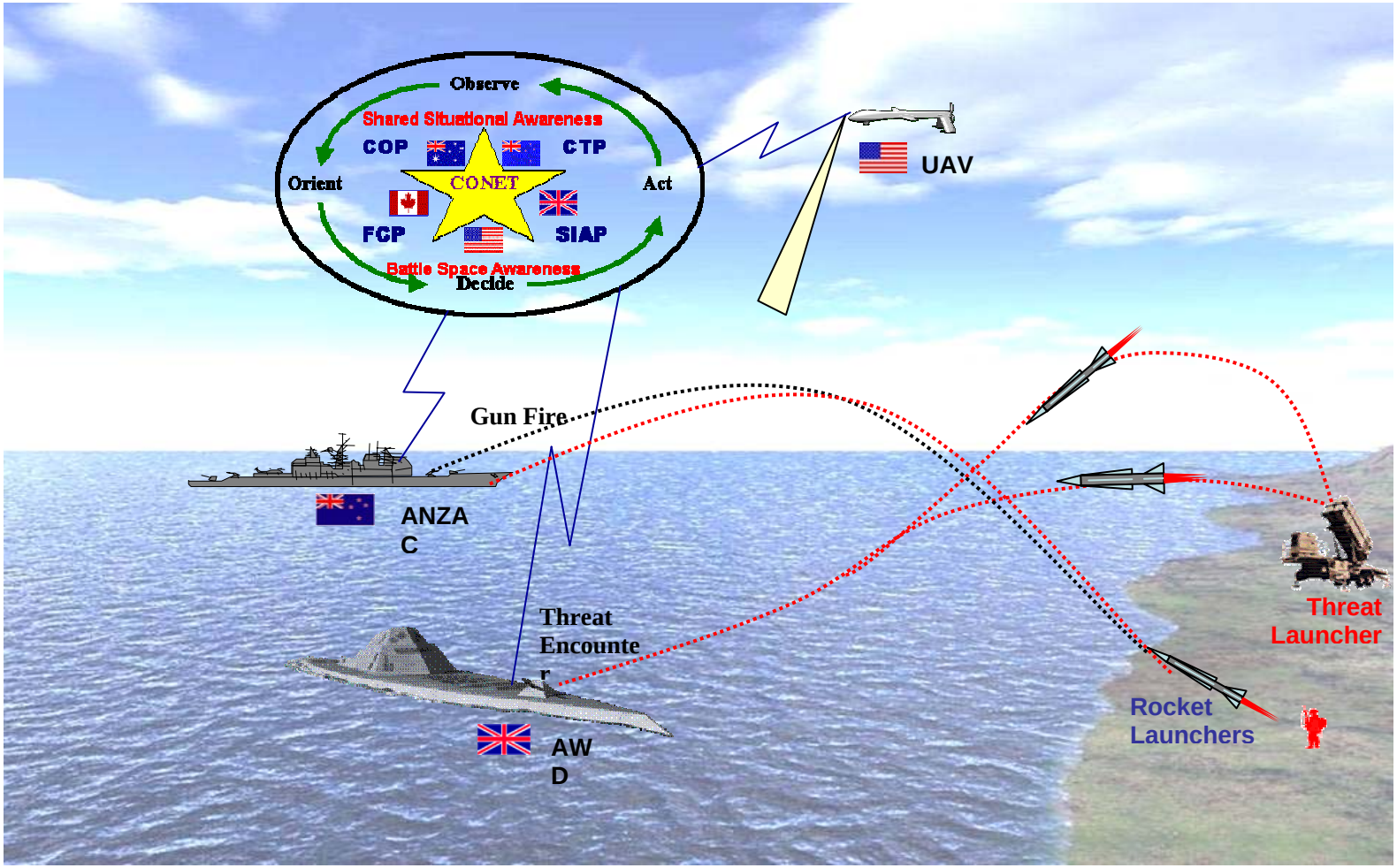


Figure A.1.4. OV-1 for Vignette 7: Naval Fires Support

A.2 Operational Node Connectivity (OV-2)

A.2.1 Product Definition

The Operational Node Connectivity Description (OV-2) graphically depicts the operational nodes/organizations with need-lines between nodes to indicate information exchange. The graphic includes operational nodes that are internal to the ESG (internal nodes) as well as operational nodes that are outside ESG (external nodes).

A.2.2 Product Purpose

The OV-2 is intended to track only information exchange between nodes; it does depict the connectivity between the nodes. It also provides characteristics of the information that is being exchanged between the nodes and describes the information that is needed to support the activities depicted by the nodes.

A.2.3 Product Overview

In Figure A2.1, the OV-2 displays the flow of data once it is received by the system. The source data is representative of the three primary vignettes for our analysis (sensor source data, ISR source data, and countermeasures source data). Upon receipt of data, the sensor grid collects and distributes the data to appropriate decision authority site, who assesses the data, respond with a set of commands to the ESG shooter grid. ESG utilizes the same paths and methods to update the collation of results of the executed command. Figures A2.2 through A2.7 represent the OV-2 diagrams for vignettes 3, 6, and 7 respectively (“As Is” and “To Be” FORCEnet representations).

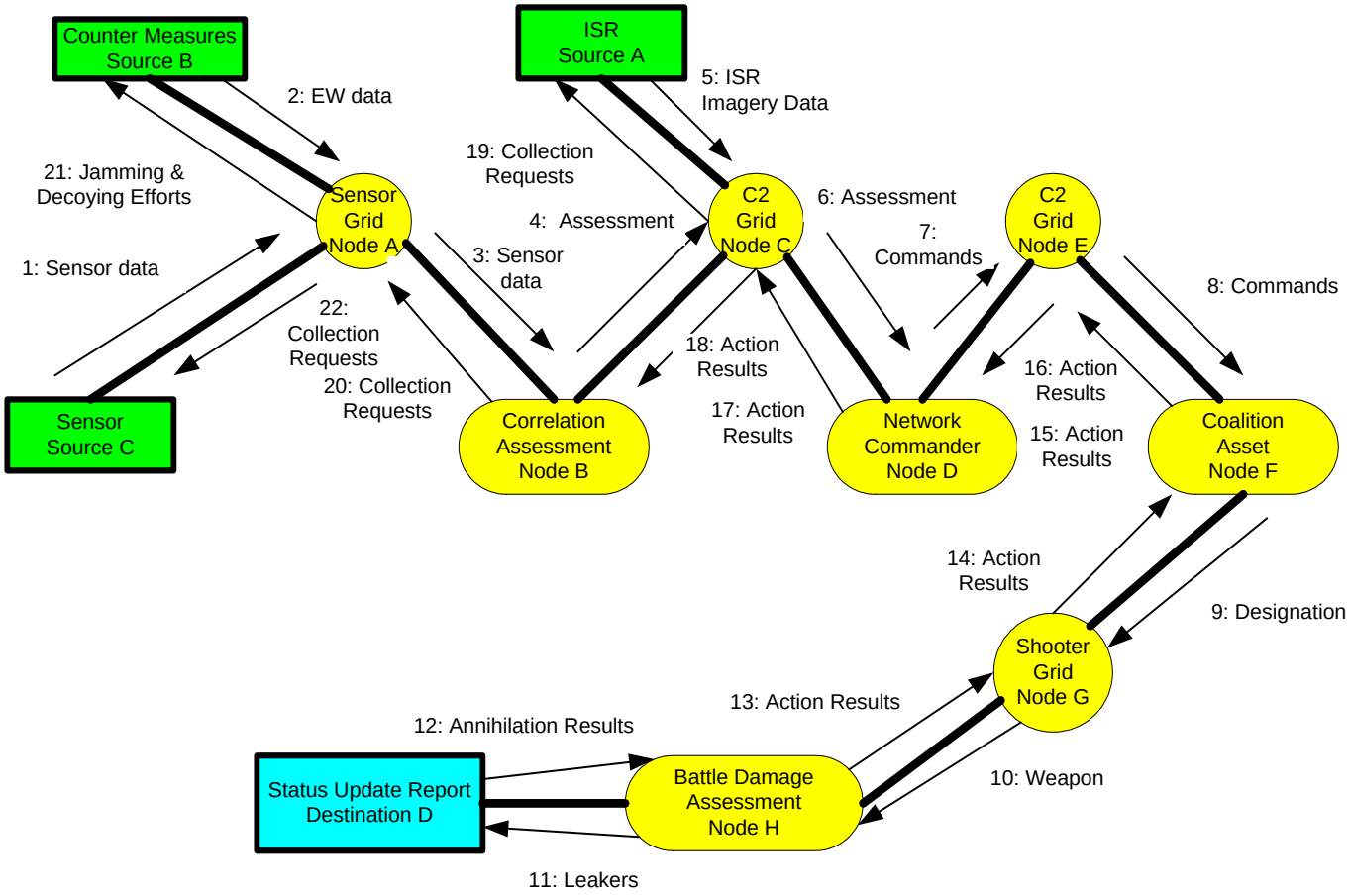


Figure A.2.1. Overall Coalition FORCEnet OV-2

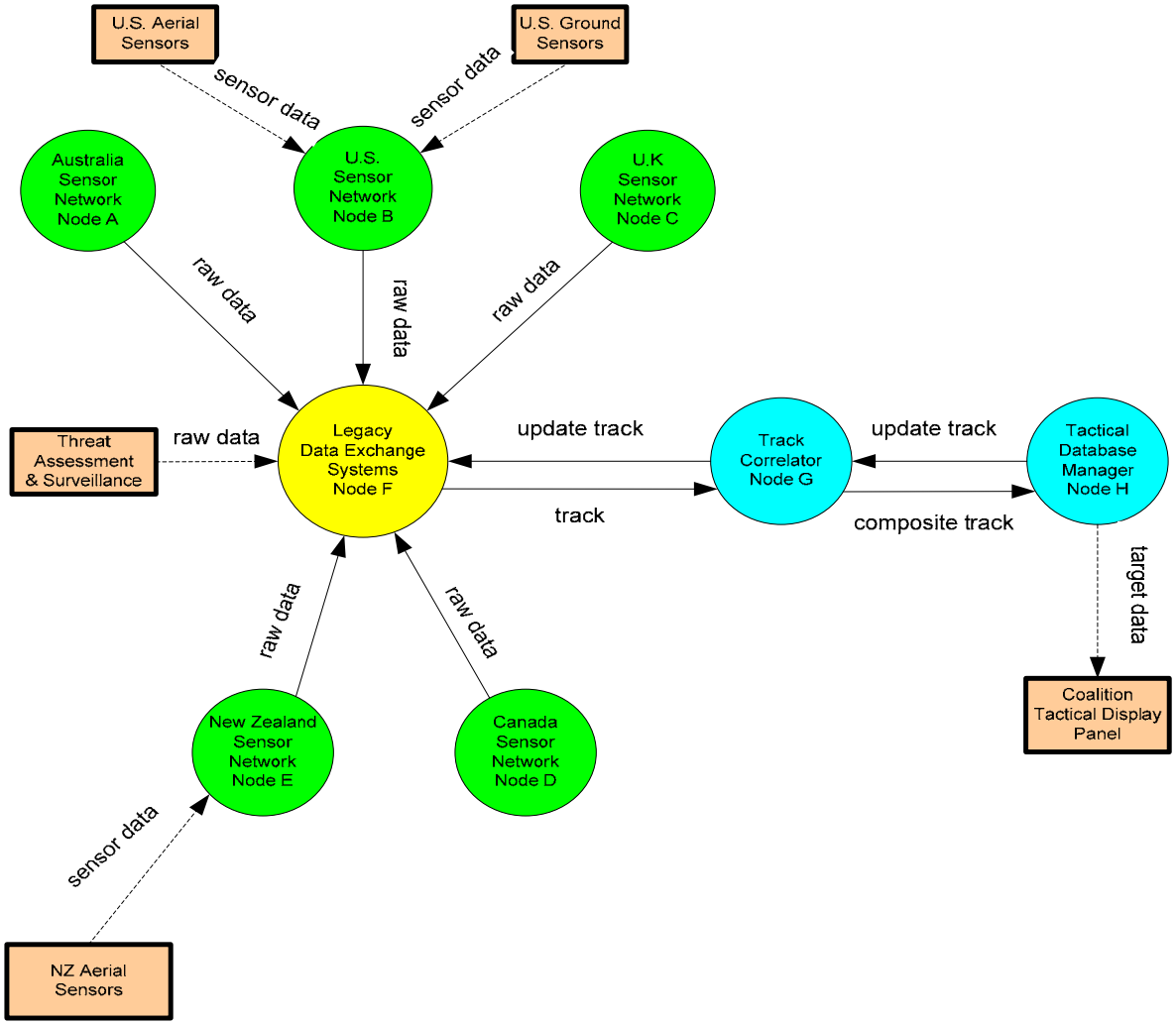


Figure A.2.2. OV-2 Diagram for Vignette 3: ASuW against the SAG Threat with Application of FORCEnet (As Is)

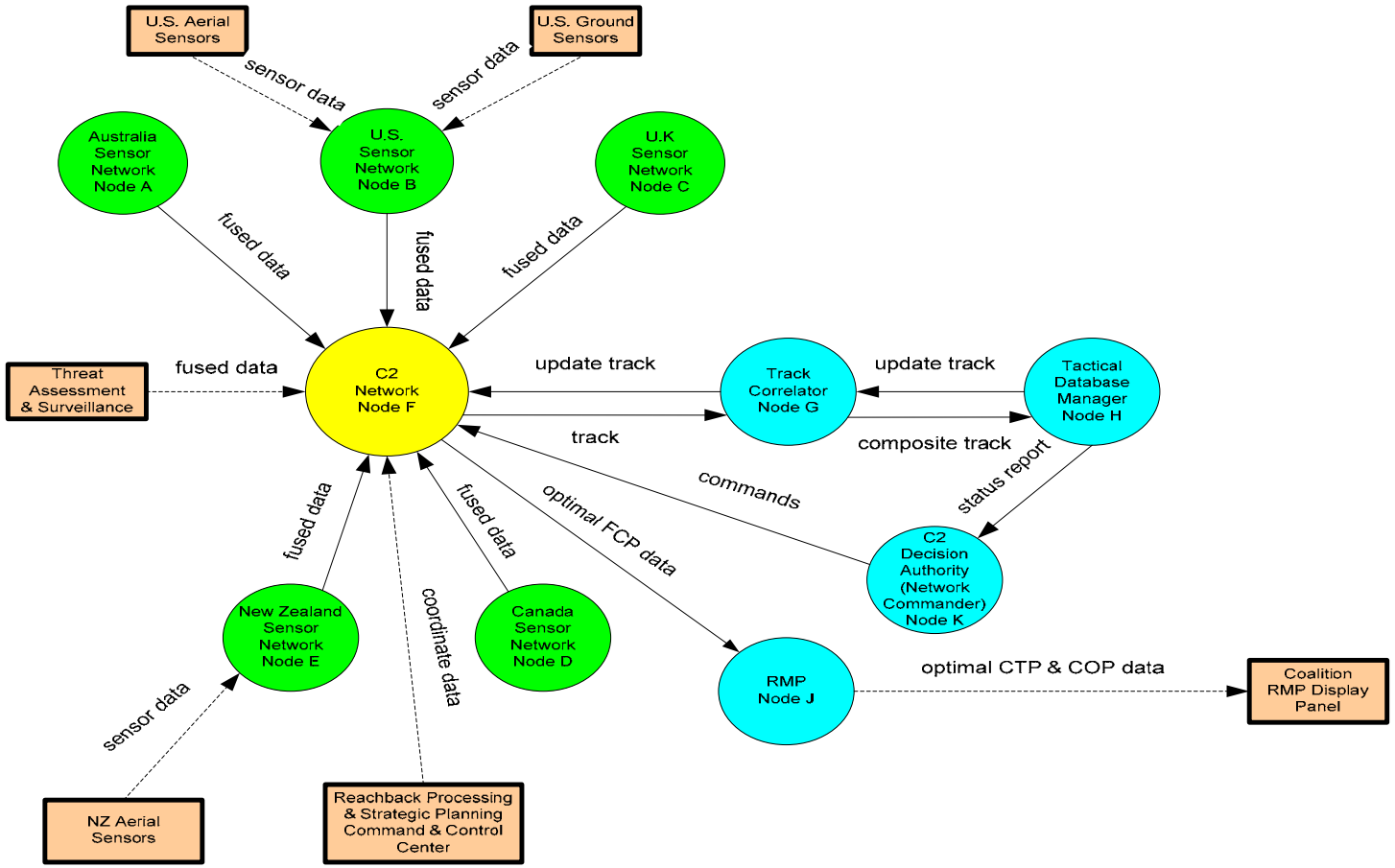


Figure A.2.3. OV-2 Diagram for Vignette 3: ASuW against the SAG Threat with Application of FORCEnet (To Be)

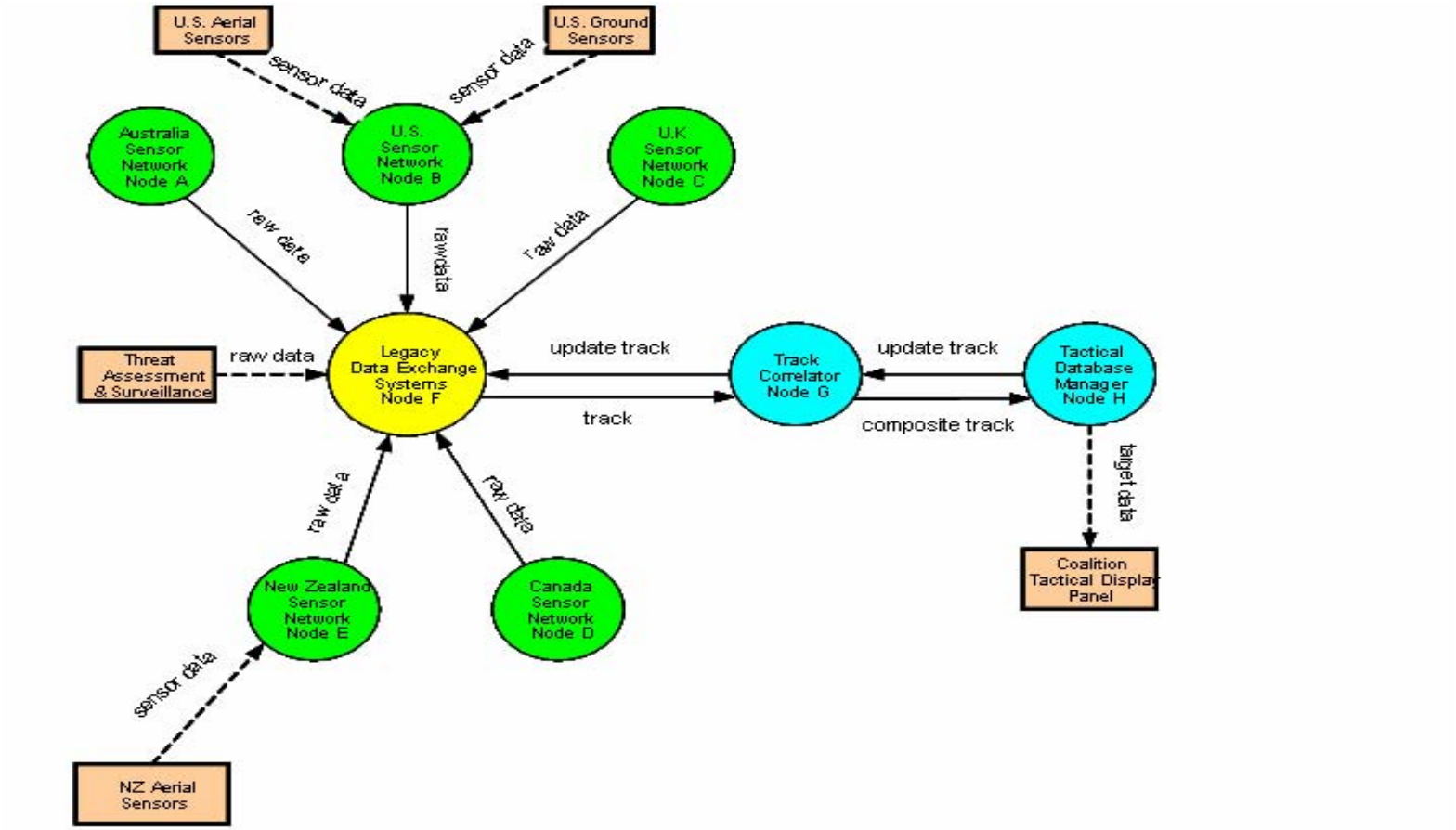


Figure A.2.4. OV-2 Diagram for Vignette 6: Amphibious Offload with Application of FORCEnet (As Is)

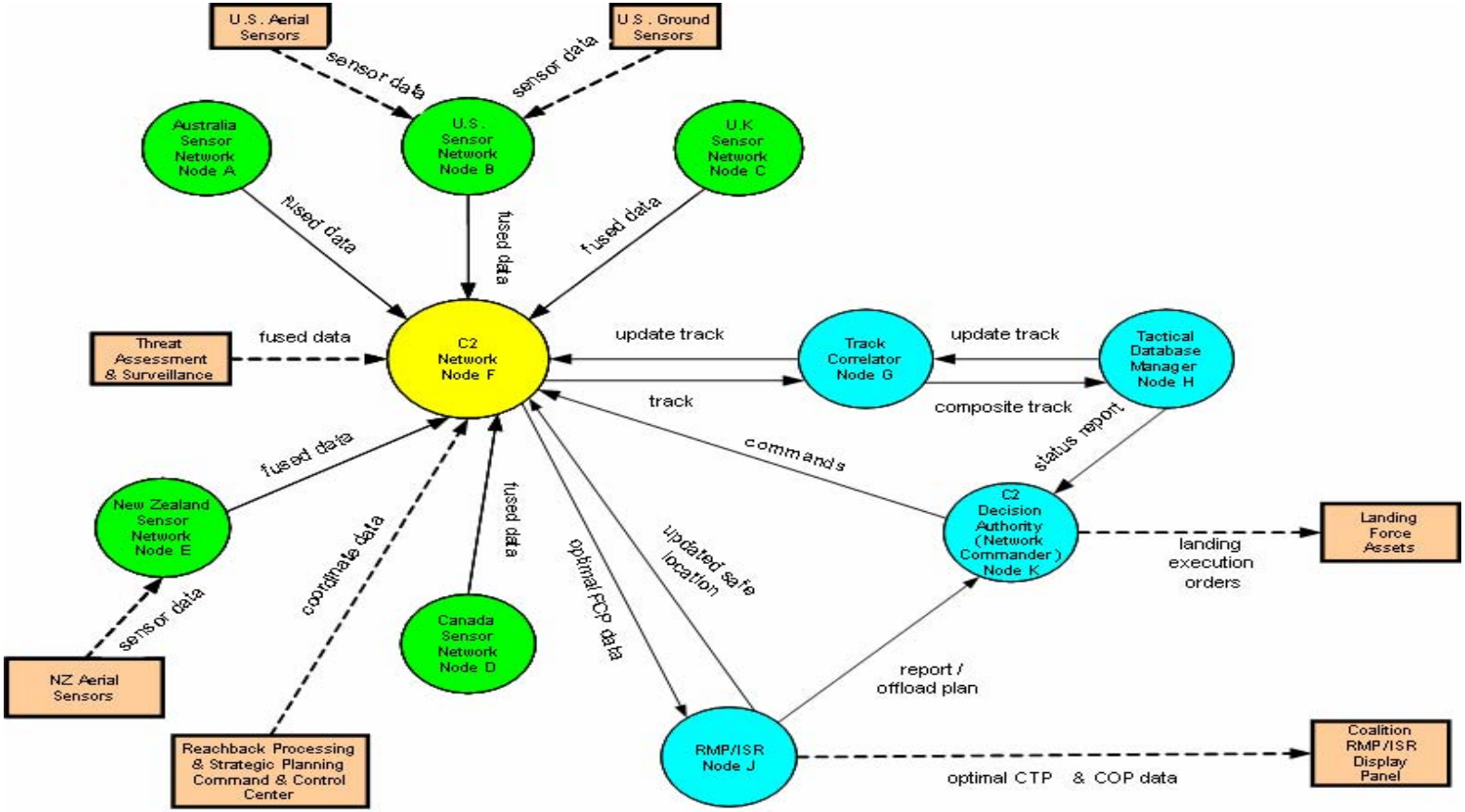


Figure A.2.5. OV-2 Diagram for Vignette 6: Amphibious Offload with Application of FORCEnet (To Be)

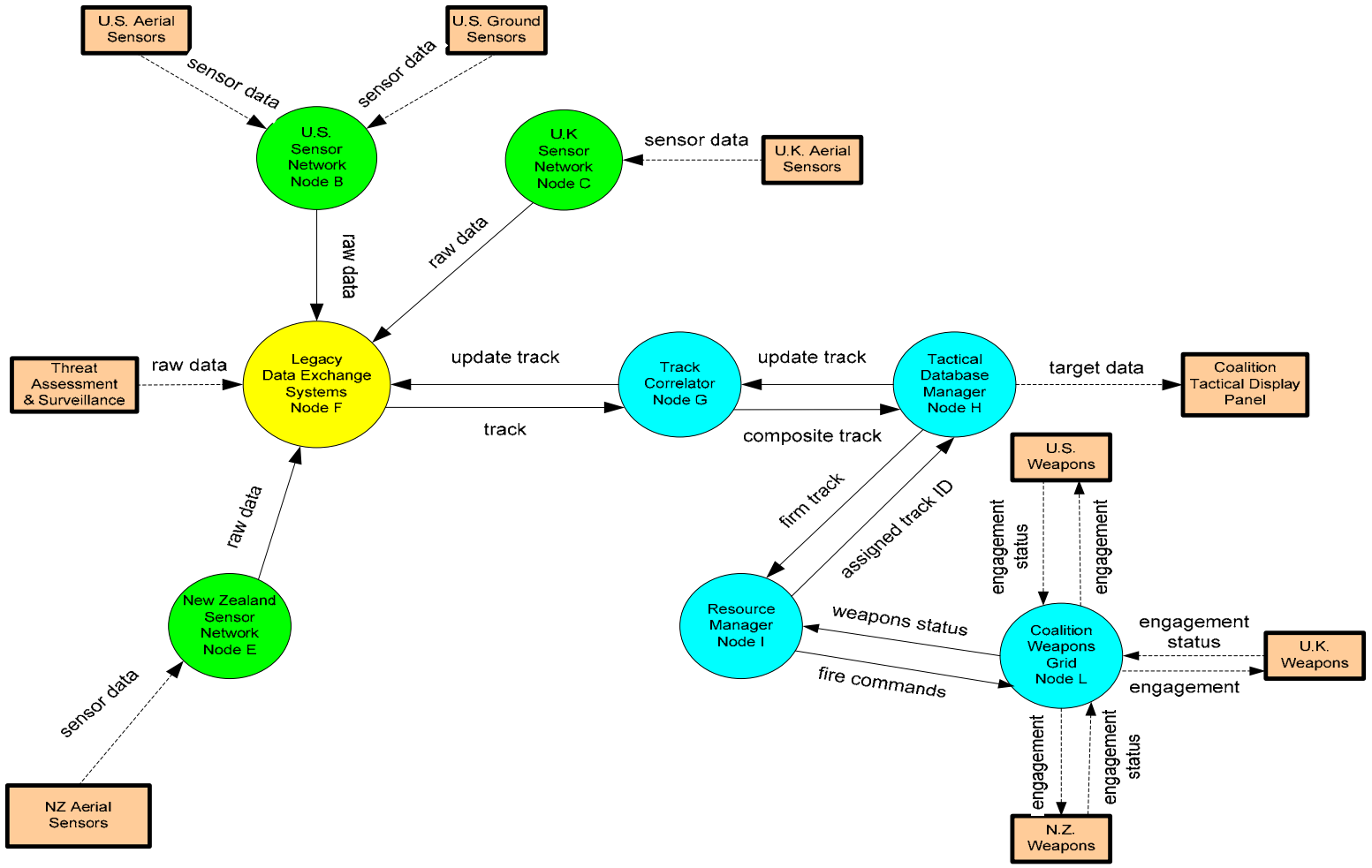


Figure A.2.6. OV-2 Diagram for Vignette 7: Naval Fires Support with Application of FORCEnet (As Is)

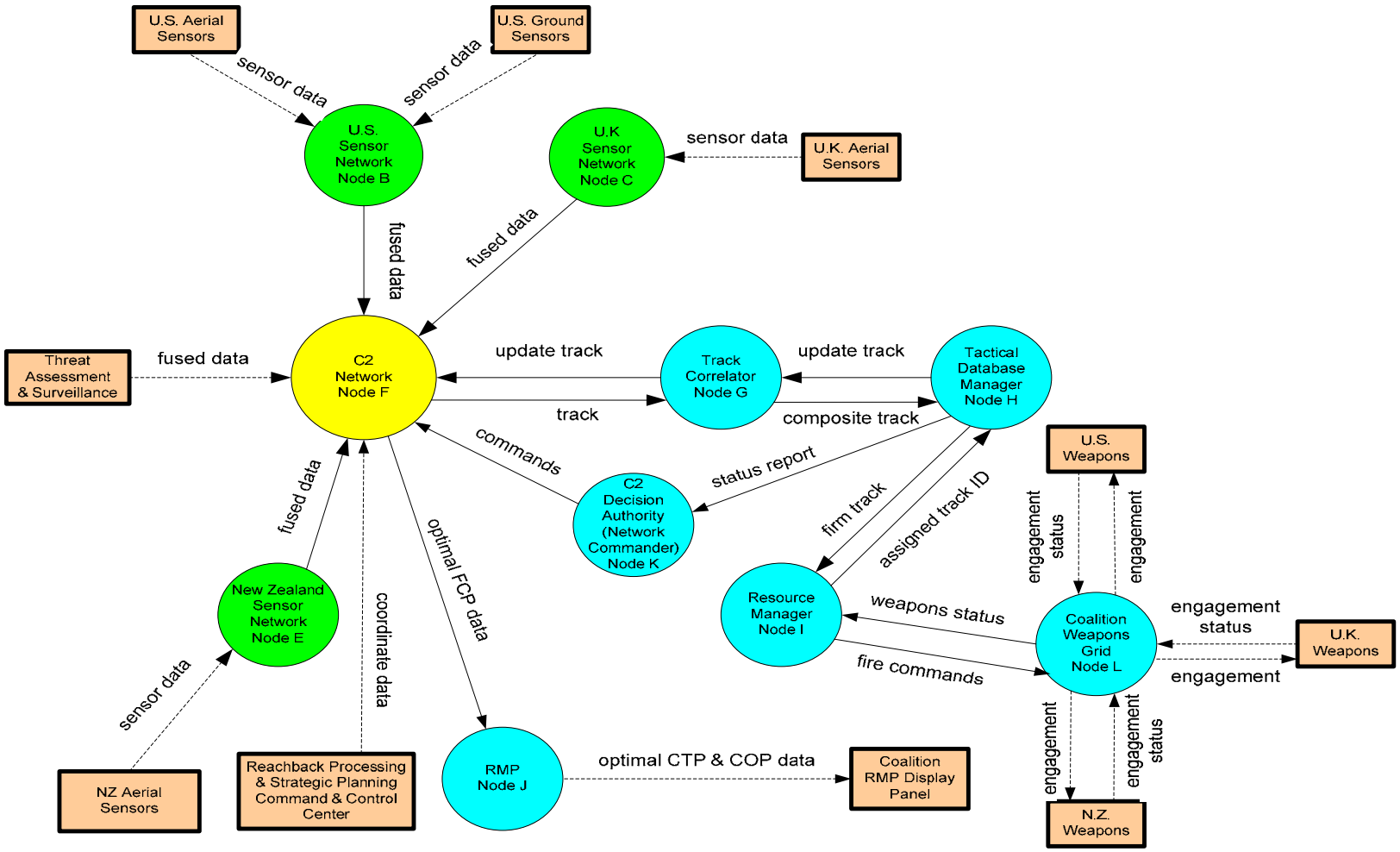


Figure A.2.7. OV-2 Diagram for Vignette 7: Naval Fires Support with Application of FORCEnet (To Be)

A.3 Operational Activity Model OV-5

A.3.1 Product Definition

The OV-5 allows one to view the hierarchical relationship amongst Functional/Operational Activities.

A.3.2 Product Purpose

OV-5 allows the architect to define and reference the connections between functions that are performed to support an operational event and the activities that are executed to carry out the function. This is especially relevant for further development of OV-5 activity models.

A.3.3 Product Overview

Figure A3.1 (As Is) and A3.2 (To Be) captures the OV-5 for vignettes 3, 6, and 7. The OV-5s are used in this model as a simple way to convey the functions and activities to the reader. It is also used as a basis for developing data flow in the model.

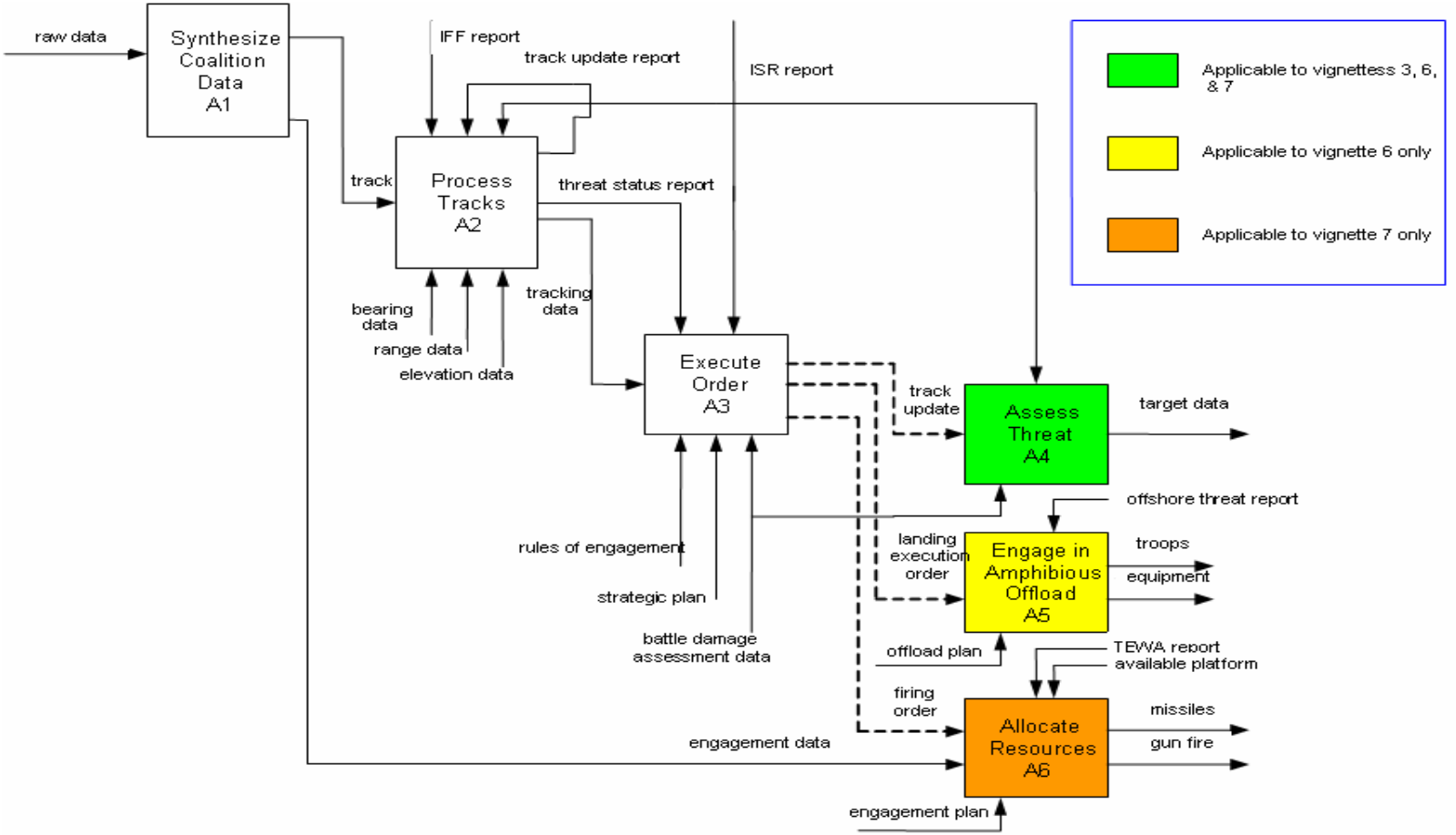


Figure A.3.1. OV-5 A0 Diagram for Vignettes 3, 6, & 7 with Application of FORCEnet (As Is)

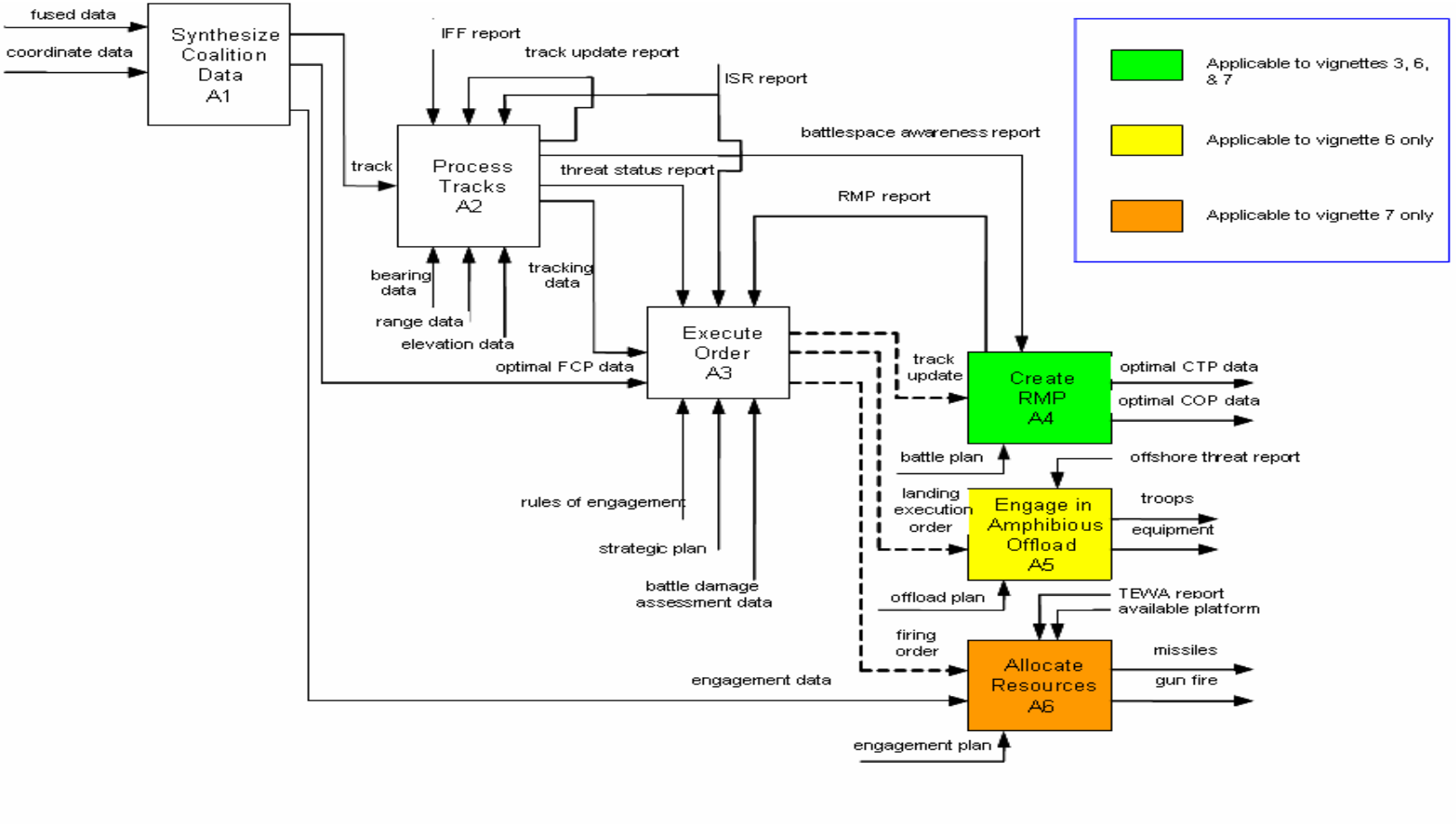


Figure A.3.2. OV-5 A0 Diagram for Vignettes 3, 6, & 7 with Application of FORCEnet (To Be)

A.4 Operational Event Trace (OV-6c)

A.4.1 Product Definition

The Operational Event Trace Diagram (OV-6c) provides a time-ordered examination of the information exchanges between participating operational nodes as a result of a particular scenario. Each event-trace diagram should have an accompanying description that defines the particular scenario or situation. It may sometimes be referred to as a sequence diagram, which shows interactions in terms of messages or information transfers between operational nodes arranged in a time-ordered sequence. This product may be used by itself, or in conjunction with an Operational State Transition Description (OV-6b) to describe dynamic behavior of the processes.

A.4.2 Product Purpose

The OV-6c is valuable for moving to the next level of detail from the initial operational concepts. This product helps to define node interactions and operational threads.

A.4.3 Product Overview

The Operational Event Trace Diagram shows operational nodes involved in the scenario by vertical swim lanes called Op Node Timelines. Inside the swim lanes are Operational Activities, which are represented by rectangles. Line symbols between the Operational Activities represent the messages or Operational Events passed between the operational nodes. The Operational Events are drawn chronologically from the top of the diagram to the bottom; the horizontal placement of the

objects is arbitrary. Figures A4.1 through A4.6 represent the OV-6c operational event trace diagrams for vignettes 3, 6, and 7 respectively ("As Is" and "To Be" FORCEnet representations).

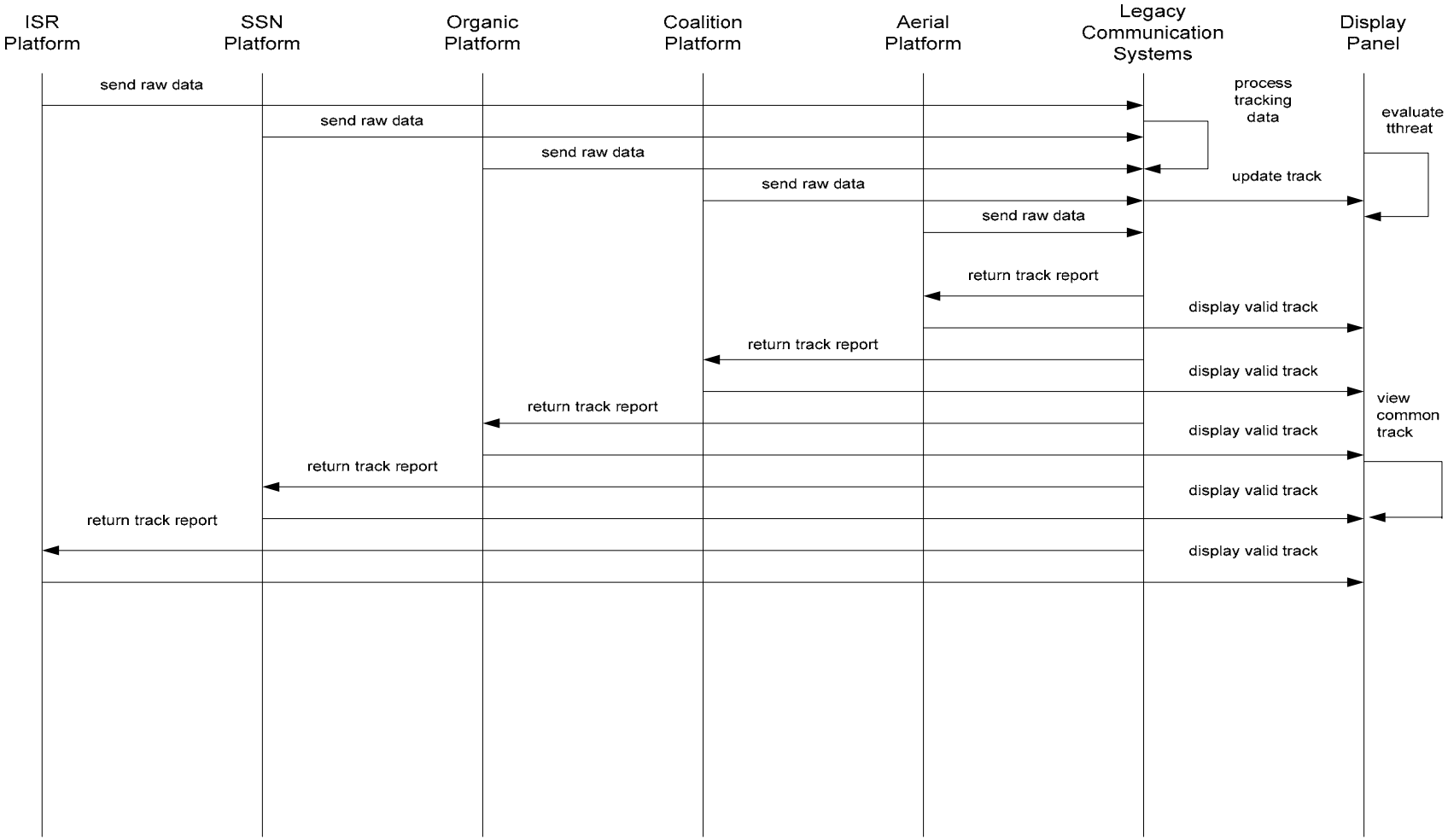


Figure A.4.1. OV-6c Diagram for Vignette 3: ASuW against the SAG Threat with Application of FORCEnet (As Is)

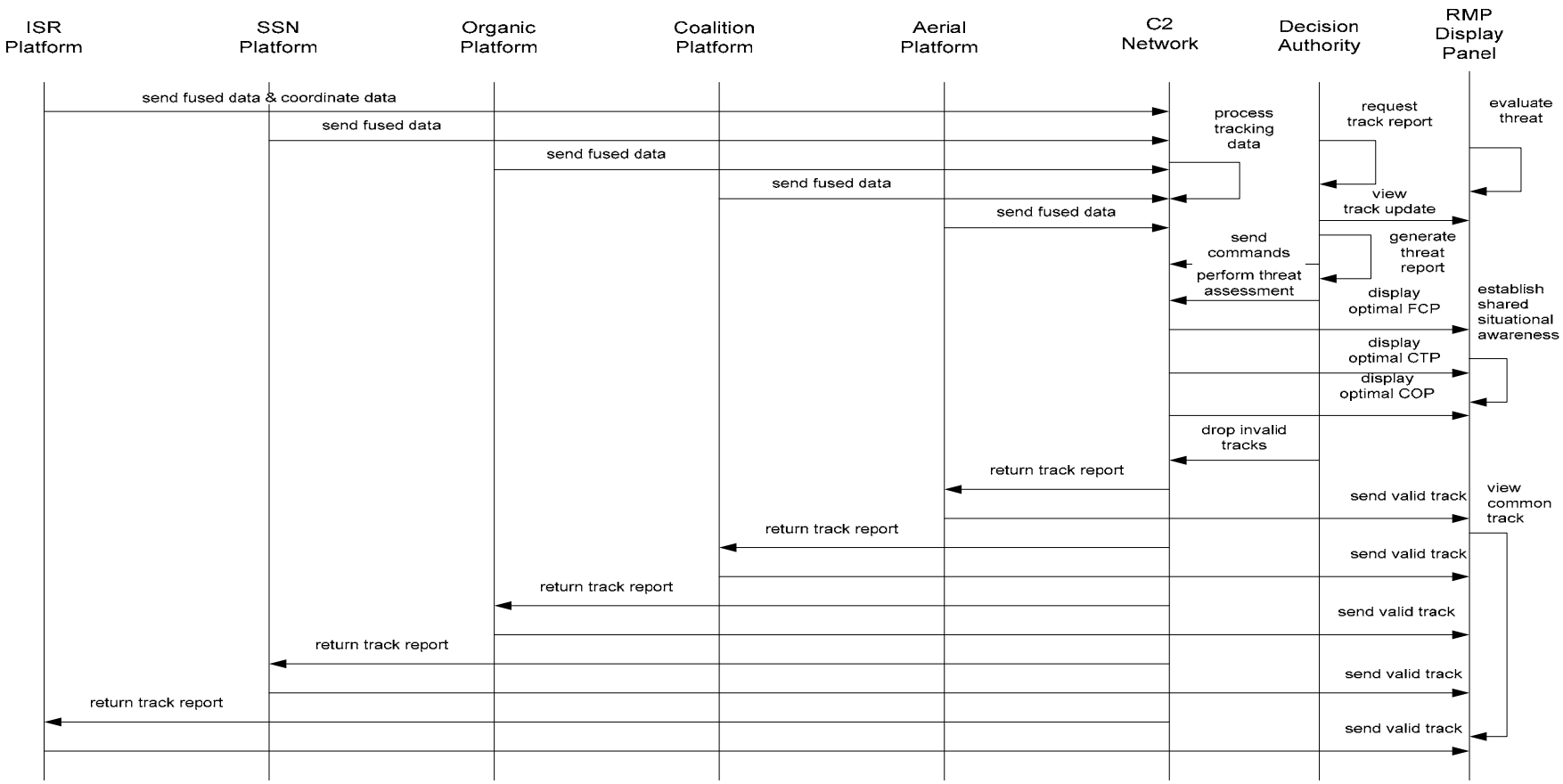


Figure A.4.2. OV-6c Diagram for Vignette 3: ASuW against the SAG Threat with Application of FORCEnet (To Be)

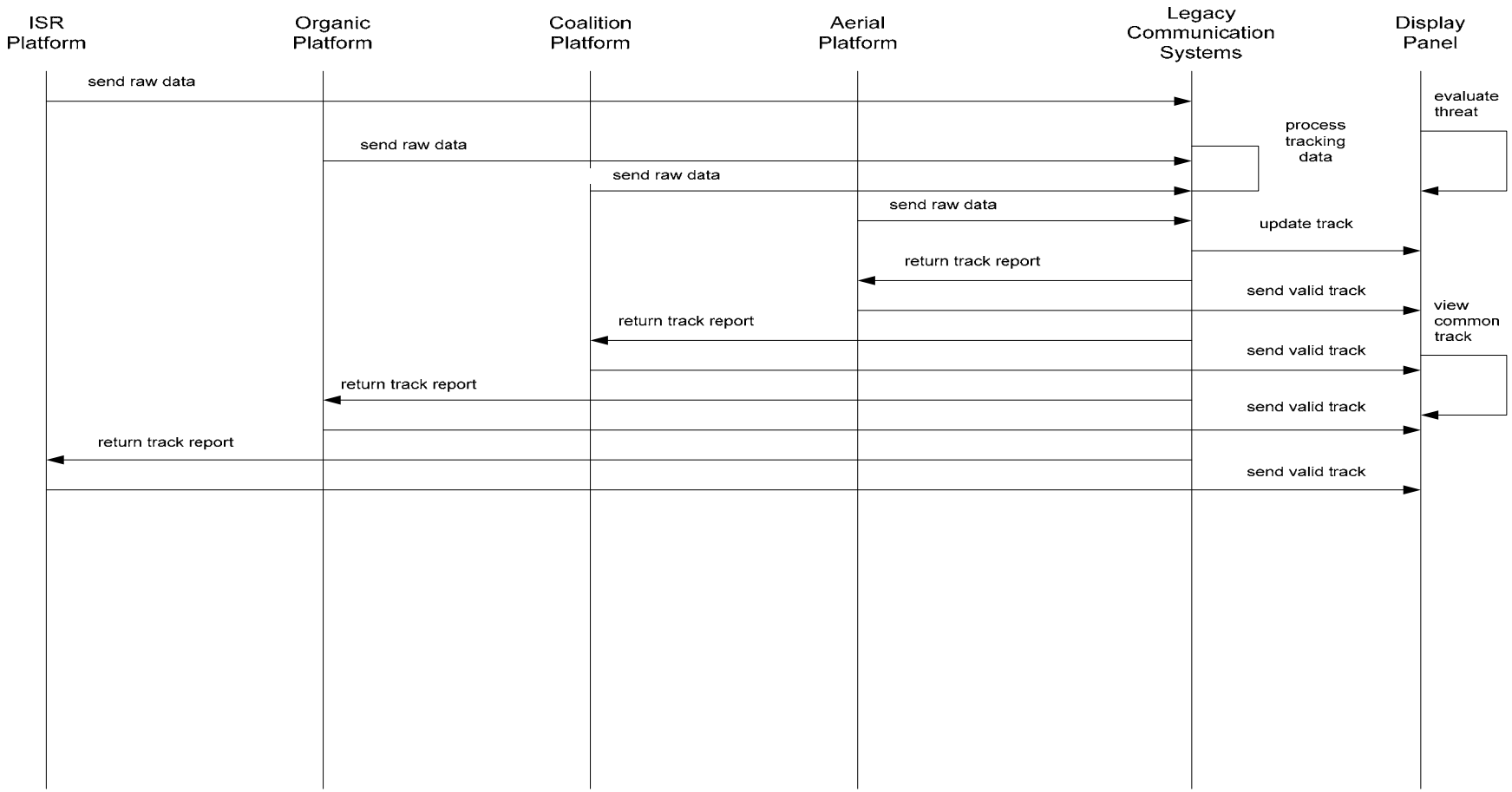


Figure A.4.3. OV-6c Diagram for Vignette 6: Amphibious Offload with Application of FORCEnet (As Is)

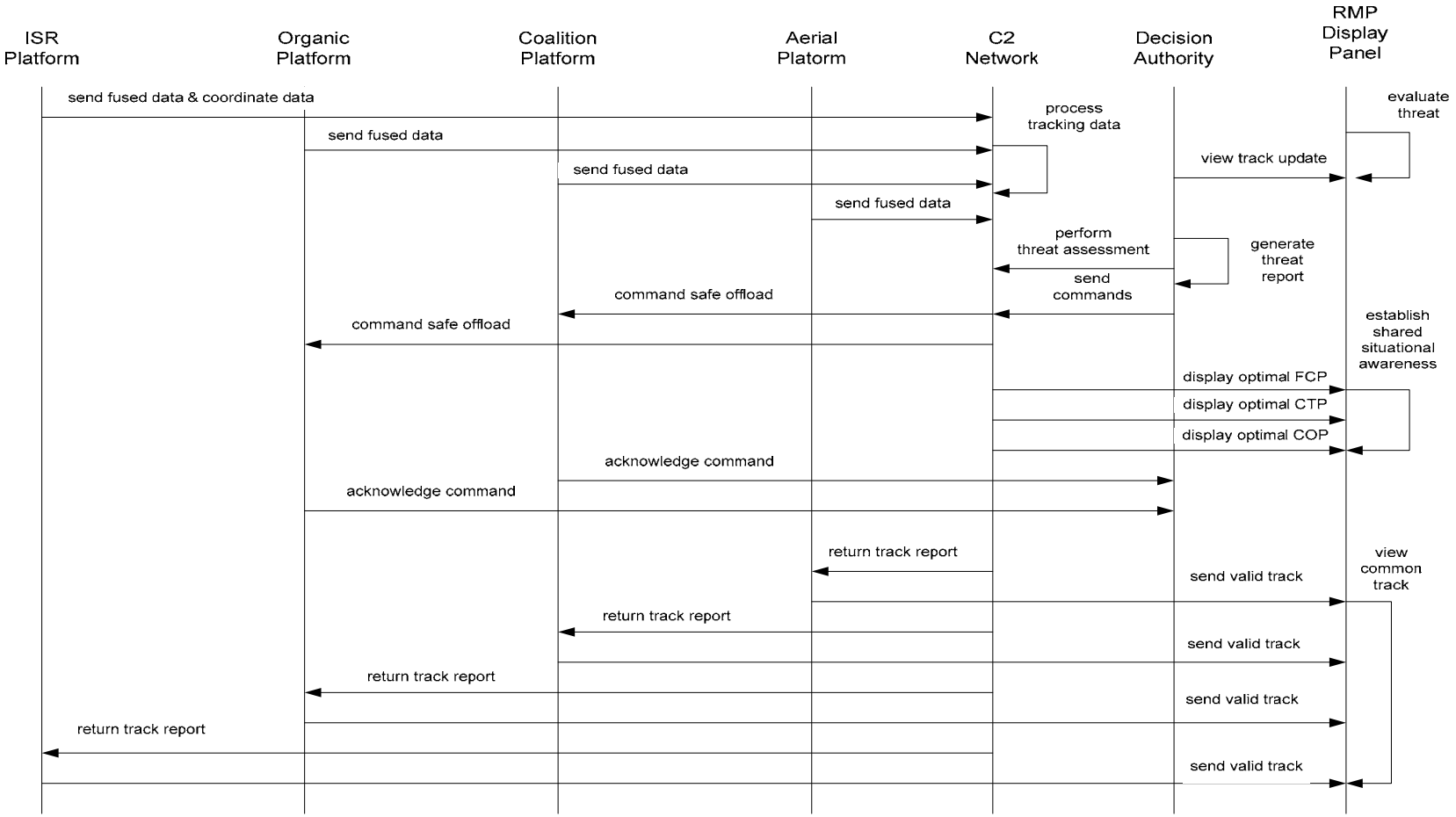


Figure A.4.4. OV-6c Diagram for Vignette 6: Amphibious Offload with Application of FORCEnet (To Be)

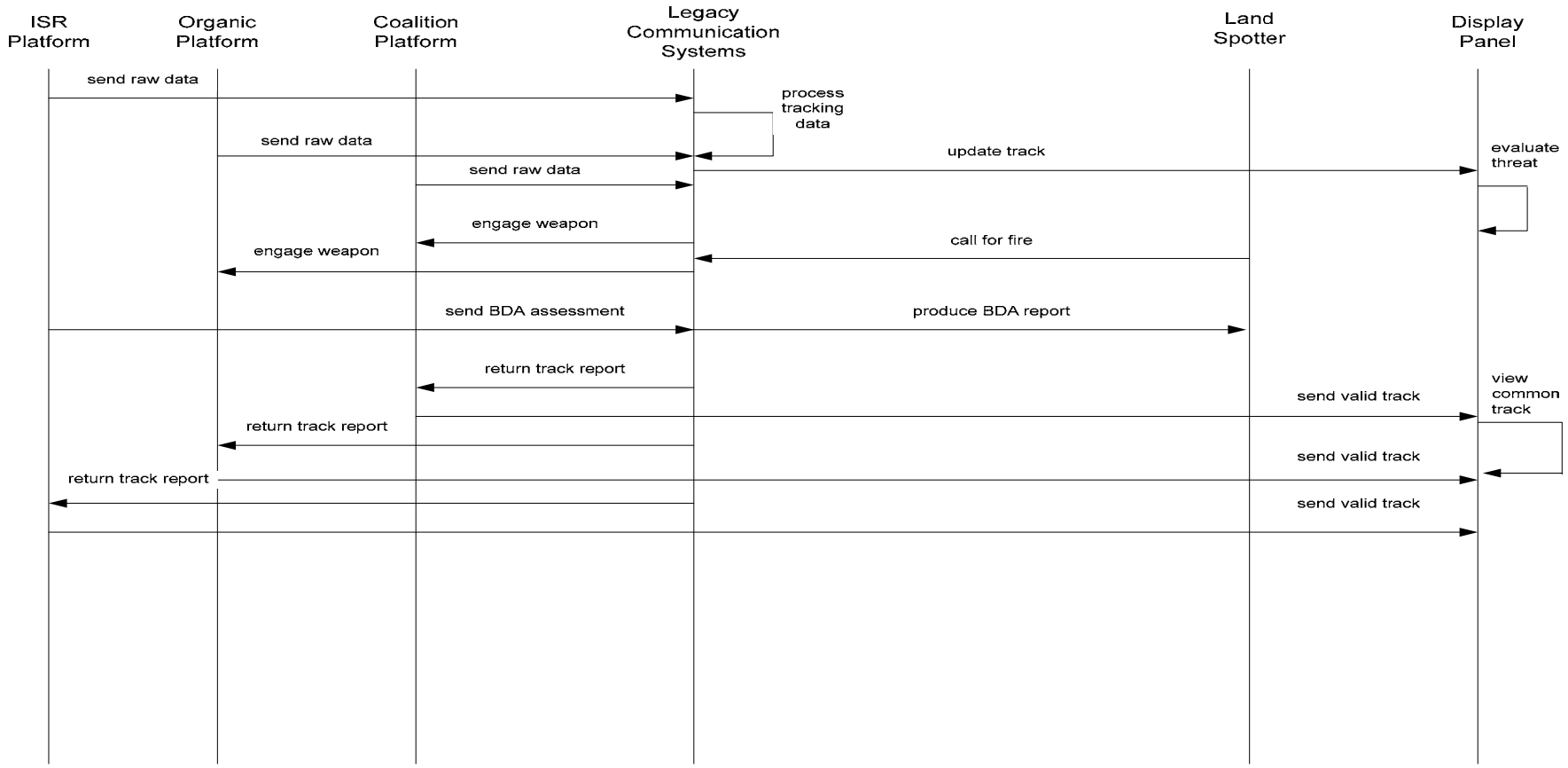


Figure A.4.5. OV-6c Diagram for Vignette 7: Naval Fires Support with Application of FORCEnet (As Is)

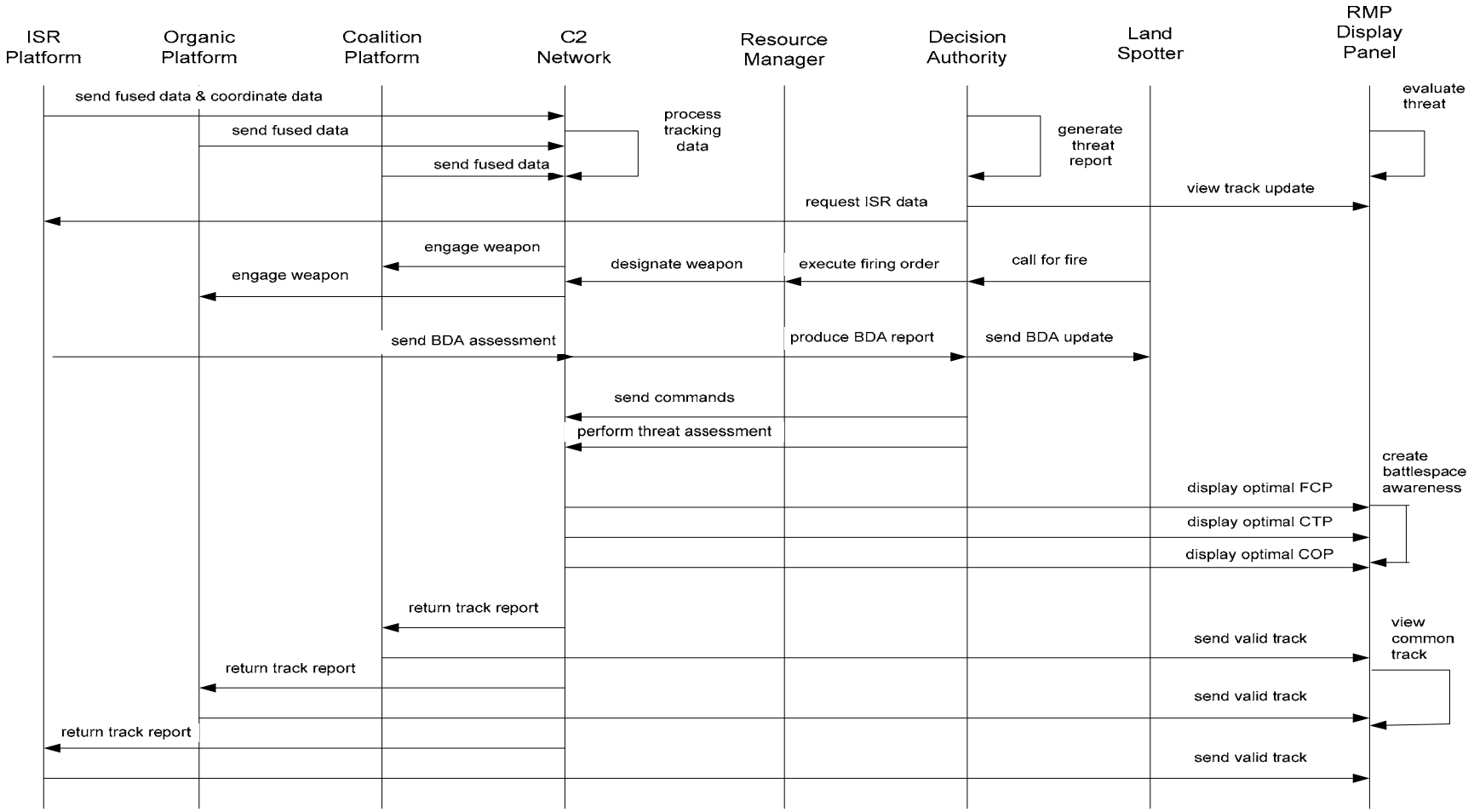


Figure A.4.6. OV-6c Diagram for Vignette 7: Naval Fires Support with Application of FORCEnet (To Be)

A.5 Systems Interface Description (SV-1)

A.5.1 Product Definition

The System Interface Description depicts system nodes and the subsystems resident within these nodes to support organizations/human roles represented by operational interfaces between systems.

A.5.2 Product Purpose

The SV-1 identifies system nodes and systems that support operational nodes. Key interfaces that cross-organizational boundaries are also identified in this product as external nodes/systems. High-level versions only show key components, with lower-level versions providing more detail as needed to describe the interfaces that are important to ESG. Detailed versions will also be developed, as needed, for use in system acquisition, requirements specification development, and for determining system interoperabilities at a finer level of technical detail.

A.5.3 Product Overview

Figure A5.1 represents the SV-1 for the projected “To Be” Coalition FORCEnet system interface description.

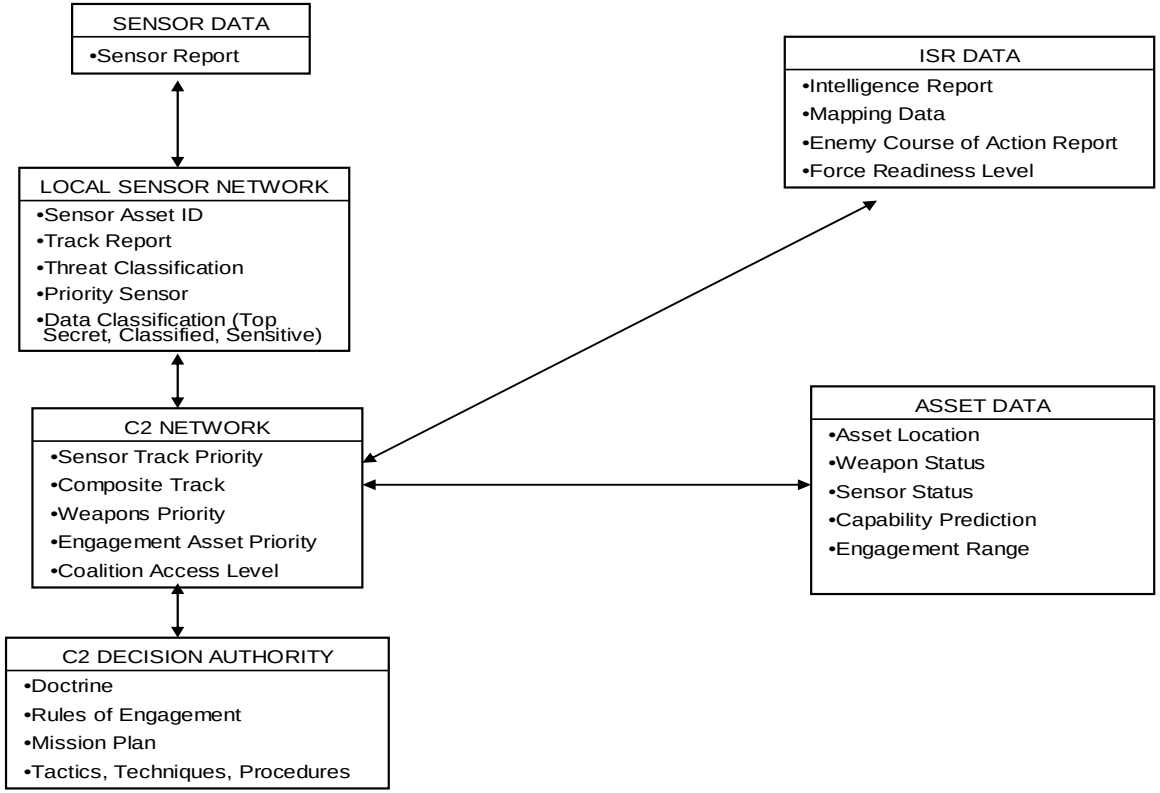


Figure A.5.1. SV-1 System Interface Diagram for Application of FORCEnet (To Be)

A.6 Systems Communications Description (SV-2)

A.6.1 Product Definition

The SV-2 documents systems, systems nodes, and system items, and their related communication lay-downs. The Systems Communications Description depicts pertinent information about communication systems, links, and networks. SV-2 documents the kinds of communications media that support the systems and their interfaces are implemented as described in SV-1. Thus, SV-2 shows the communications details of SV-1 interfaces that automate aspects of the need-lines represented in OV-2.

A.6.2 Product Purpose

SV-2 can be used to document how interfaces (described in SV-1) are supported by physical media. This kind of communications media support information is critical in performing certain infrastructure and system acquisition decisions.

A.6.3 Product Overview

SV-2 documents the specific communications links or communications networks (e.g., Intelink or Joint Worldwide Intelligence Communications System [JWICS]) and the details of their configurations through which systems interface. While SV-1 depicts interfaces between systems or system nodes, SV-2 contains a detailed description of how each SV-1 interface is implemented (e.g., composing parts of the implemented interface including communication systems, multiple communication

links, communications networks, routers, and gateways). Figure A6.1 and A6.2 represent the "As IS" and "To Be" SV-2 system communications descriptions for Coalition FORCEnet.

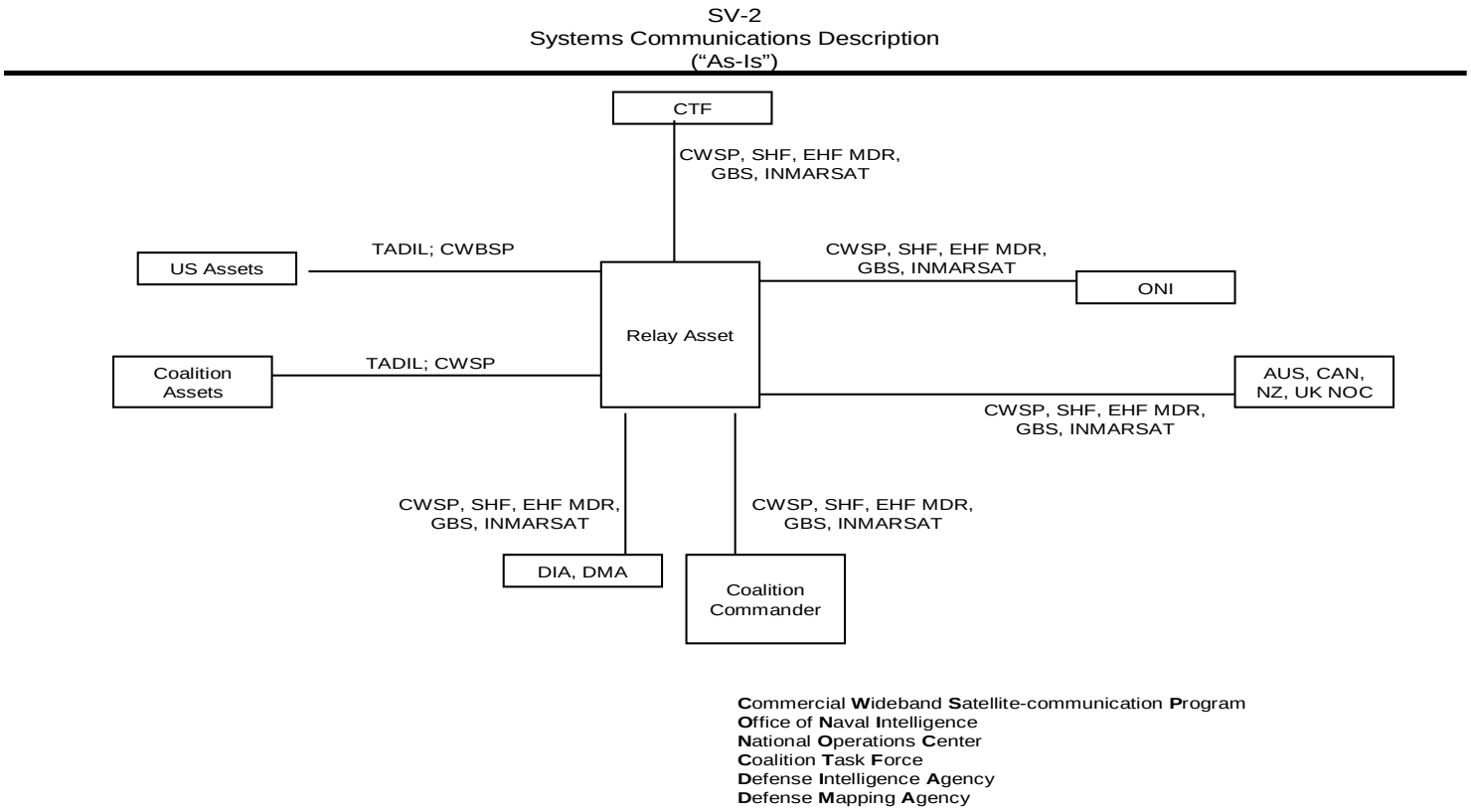
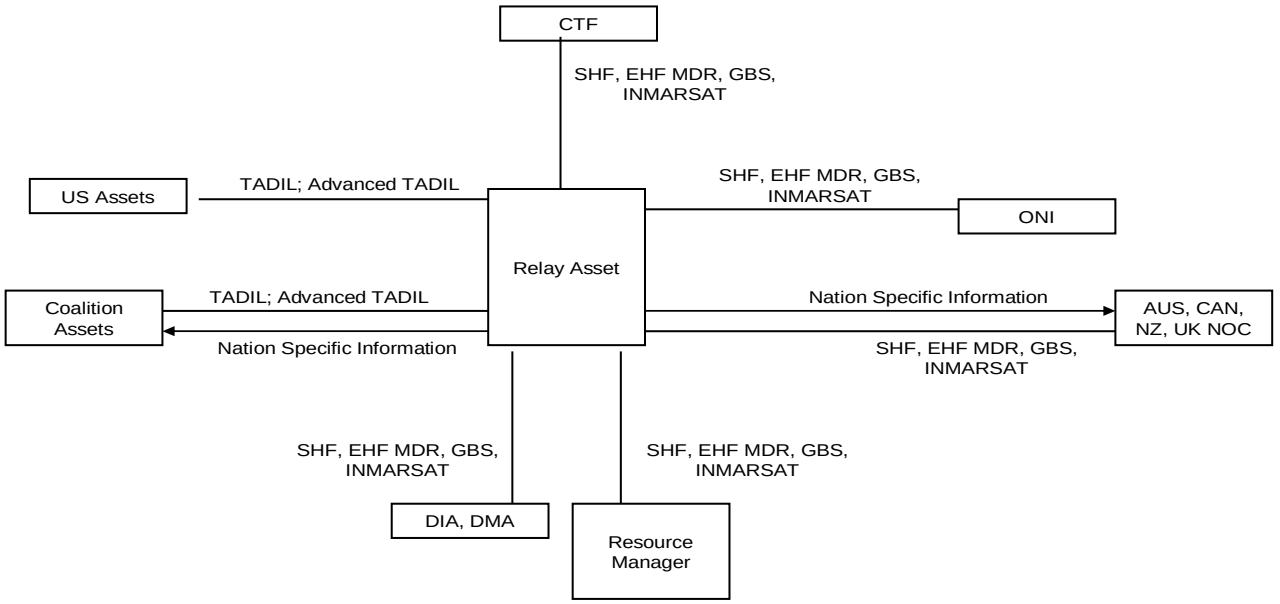


Figure A.6.1. SV-2 System Communications Description for Application of FORCEnet (As Is)

SV-2
Systems Communications Descriptions
("To-Be")



All communication networks and links will have the capability to receive and transmit SCI, Top Secret, Secret, and Confidential data on an as needed basis securely and reliably.

Commercial **W**ideband **S**atellite-communication **P**rogram
Office of **N**aval **I**ntelligence
National **O**perations **C**enter
Coalition **T**ask **F**orce
Defense **I**ntelligence **A**gency
Defense **M**apping **A**gency

Figure A.6.2. SV-2 System Communications Description for Application of FORCEnet (To Be)

A.7 Systems Functional Description (SV-4)

A.7.1 Product Definition

The SV-4 documents system functional hierarchies and system functions, and the system data flows between them. Although there is a correlation between Operational Activity Model (OV-5) or business-process hierarchies and the system functional hierarchy of SV-4, it need not be a one-to-one mapping, hence, there is a need for the Operational Activity to Systems Function Traceability Matrix (SV-5), which provides that mapping.

A.7.2 Product Purpose

The SV-4 depicts which systems support the activities depicted in the OV-5. This diagram is similar to a node tree or functional hierarchy diagram.

A.7.3 Product Overview

Figure A7.1 and A7.2 represent the “As Is” and “To Be” SV-4 system functional descriptions for Coalition FORCEnet. These SV-4s show which subsystems support the activities depicted in the OV-5. It depicts how the sensor data, command decisions, and weapons engagement feedback are distributed through the collaborative environment.

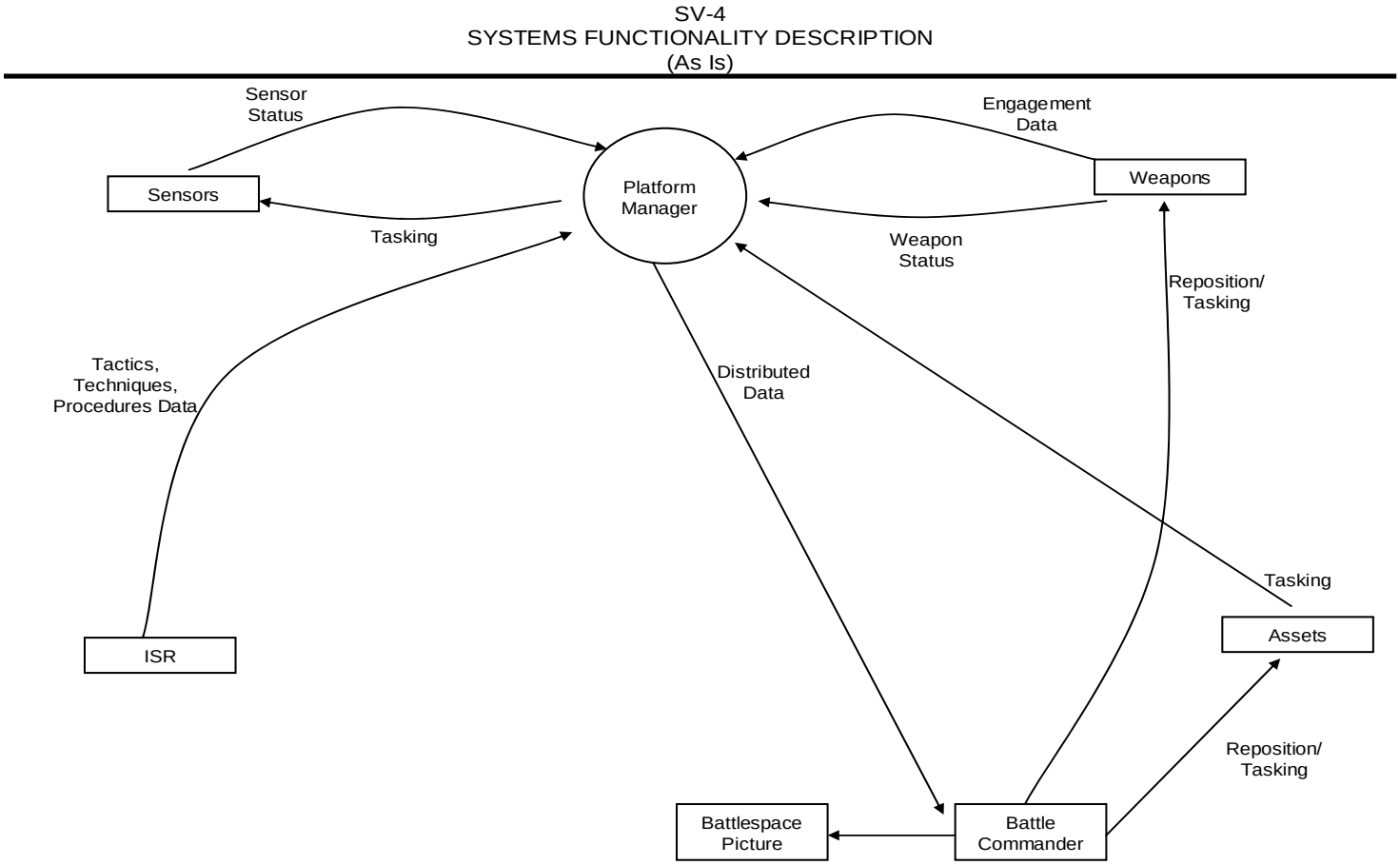


Figure A.7.1. SV-4 for Application of FORCEnet (As Is)

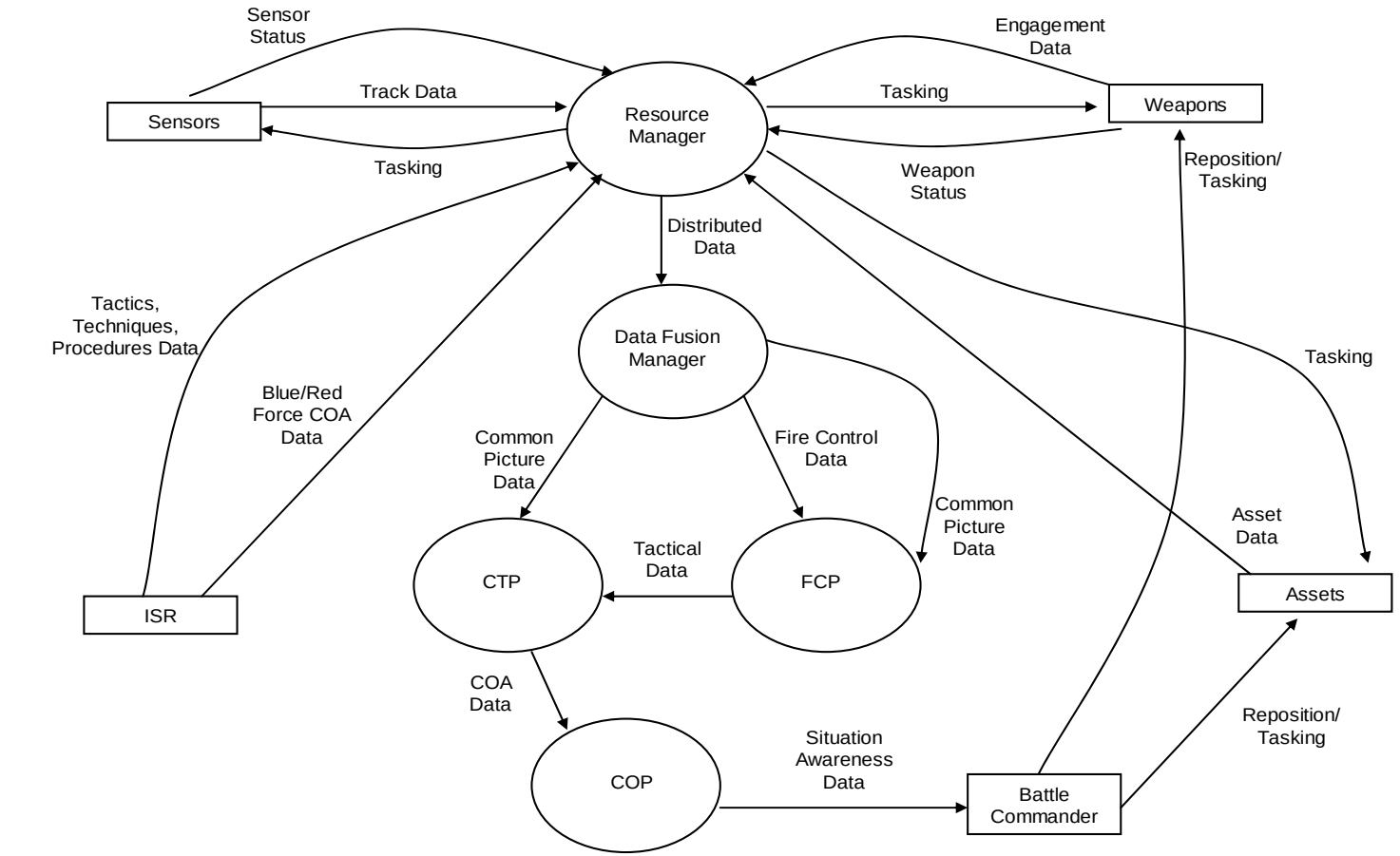


Figure A.7.2. SV-4 for Application of FORCEnet (To Be)

A.8 Operational Activity to Systems Function Traceability Matrix (SV-5)

A.8.1 SV-5 Product Definition

Operational Activity to Systems Function Traceability Matrix is a specification of the relationships between the set of operational activities applicable to architecture and the set of system functions within that architecture.

A.8.2 SV-5 Product Purpose

The SV-5 depicts the mapping of operational activities to system functions and thus identifies the transformation of an operational need into a purposeful action performed by a system.

The SV-5 can be extended to depict the mapping of capabilities to operational activities, operational activities to system functions, system functions to systems, and thus relates the capabilities to the systems that support them. Such a matrix allows decision makers and planners to quickly identify stovepiped systems, redundant/duplicative systems, gaps in capability, and possible future investment strategies all in accordance with the time stamp given to the architecture. SV-5 correlates capability requirements that would not be satisfied if a specific system were not fielded to a specific DoD unit.

A.8.3 Product Overview

Figure A8.1 and A8.2 represent the “As Is” and “To Be” SV-5 for Coalition FORCEnet. The SV-5 maps operational capabilities to system functions within the Coalition FORCEnet. Activity in the OVs and functions in the SVs refer to

essentially the same kind of thing. Both activities and functions are tasks that accept inputs and develop outputs. The activities are drawn from the OV-5 and the OV-6C whereas the system functions are drawn from the SV-4.

SV-5
Operational Activity to Systems Function Traceability Matrix
(As Is)

Operational Activities (OV-5) / System Functions (SV-4)	Raw Data	Engagement Data	Track	IFF Report	Track Update Report	Threat Status Report	Tracking Data	Elevation Data	Range Data	Bearing Data	ISR Report	Track Update	Landing Executing Order	Battle Damage Assessment Data	Strategic Plan	Rules of Engagement	Firing Order	Target Data	Offshore Threat Report	Troops	Equipment	Offload Plan	Available Platform	Missiles	Gun Fire	Engagement Plan	TEWA Report
Platform Manager	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x

Using OV-5 A0 diagram for vignettes 3,6,7 with Fn Level 0

Figure A8-1. SV-5 for Application of FORCEnet (As Is)

SV-5
Operational Activity to Systems Function Traceability Matrix
(To Be)

Operational Activities (OV-5) / System Functions (SV-4)	Fused Data	Coordinated Data	Engagement Data	IFF Report	Track Update Report	Threat Status Report	Tracking Data	Elevation Data	Range Data	Bearing Data	ISR Report	Track Update	Landing Executing Order	Battle Damage Assessment Data	Strategic Plan	Rules of Engagement	Firing Order	Optimal CTP Data	Optimal COP Data	Troops	Equipment	Offload Plan	Available Platform	Missiles	Gun Fire	Engagement Plan	TEWA Report	Track	Battlespace Awareness Report	RMP Report	Optimal FCP Data	Offshore Threat Report	Battle Plan
Platform Manager	X	X	X	X	X	X	X	X	X	X	X	X		X				X	X	X	X	X						X	X		X	x
Data Fusion Manager	X	X	X			X					X		X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X
FCP	X														X		X	X	X	X	X		X	X	X	X	X			X	X		
CTP	X														X			X	X	X	X			X			X			X	X		
COP	X	X	X												X				X			X				X			X	X		X	X

Using OV-5 A0 diagram for vignettes 3,6,7 with Fn Level 4

Figure A.8.2. SV-5 for Application of FORCEnet (To Be)

A.9 Systems Data Exchange Matrix (SV-6)

A.9.1 Product Definition

The Systems Data Exchange Matrix specifies the characteristics of the system data exchanged between systems. This product focuses on automated information exchanges that are implemented in systems.

A.9.2 Product Purpose

System data exchanges express the relationship across the three basic architecture data elements of an SV (systems, system functions, and system data flows) that focuses on specific aspects of the system data flow and content.

A.9.3 Product Overview

The SV-6 for Coalition FORCEnet describes in tabular format (Table A.9.1), the data exchanged between systems.

	Input							Output					
System or System Element	**Source**	**Content**	**Media**	**Data Media Format**	**Security Level**	**Frequency**	**System Functions**	**Destination**	**Content**	**Media**	**Data Media Format**	**Security Level**	**Frequency**
Sensor Data	Radar	Track Data	RF	Encrypted IP	Secret	X	Integrated Fire Control	Wpn Sys	Eng Order	Data Packet	Encrypted IP	Secret	S
	Satellite	ISR	RF	Encrypted IP	Secret	X		Wpn Sys	Eng Order	Data Packet	Encrypted IP	Secret	S
	Visual	ISR	RF/IR	Encrypted IP	Secret	X		Wpn Sys	Eng Order	Data Packet	Encrypted IP	Secret	S
	UAV	ISR	RF/IR	Encrypted IP	Secret	X		Wpn Sys	Eng Order	Data Packet	Encrypted IP	Secret	S
	Aircraft	ISR / Track	RF	Encrypted IP	Secret	X		Wpn Sys	Eng Order	Data Packet	Encrypted IP	Secret	S
Composite Track	Processed Data	Track Data	RF/IR	Encrypted IP	Secret	X	Automated Battle Management Aids (ABMA)	Coalition ESG	Common Operating Picture (COP)	Orders	Encrypted IP	Secret	X / K / Ka
Composite ID	Track Prosecution	IFF Data	RF	Encrypted IP	Secret	X							
HQ	Cmd Data	Eng Rules	RF/IR	Encrypted IP	Secret	X							
Weapons	Wpn Group	Assets	RF	Encrypted IP	Secret	X							
Sensor Data	Radar	Track Data	RF	Encrypted IP	Secret	Ku	Composite Tracking	COP	Track Data	Track File Data	Encrypted IP	Secret	Ku
	Satellite	ISR	RF	Encrypted IP	Secret	Ku		ABMA	Track Data	Track File Data	Encrypted IP	Secret	Ku
	Visual	ISR	RF/IR	Encrypted IP	Secret	Ku							
	UAV	ISR	RF/IR	Encrypted IP	Secret	Ku							
	Aircraft	ISR / Track	RF	Encrypted IP	Secret	Ku							

Table A.9.1. Coalition ESG FORCEnet SV-6

System or System Element			Input				System Functions			Output			
	Source	Content	Media	Data Media Format	Security Level	Frequency		Destination	Content	Media	Data Media Format	Security Level	Frequency
Sensor Data	Radar	Track Data	RF	Encrypted IP	Secret	Ku	Composite ID of Friend and Foe	COP	Track Data	Track File Data	Encrypted IP	Secret	Ku
	Satellite	ISR	RF	Encrypted IP	Secret	Ku		ABMA	Track Data	Track File Data	Encrypted IP	Secret	Ku
	Visual	ISR	RF/IR	Encrypted IP	Secret	Ku							
	UAV	ISR	RF/IR	Encrypted IP	Secret	Ku							
	Aircraft	ISR / Track	RF	Encrypted IP	Secret	Ku							
	Composite Track	Track Data	RF/IR	Encrypted IP	Secret	Ku / Ka	Common/Single Integrated Picture						
	Common ID	Track Prosecution	RF/IR	Encrypted IP	Secret	Ku / Ka							

Table A.9.1. Coalition ESG FORCEnet SV-6 (cont.)

APPENDIX B: DETAILED FORECENET CAPABILITIES MATRIX[34]

[34] Additional capabilities derived from TTCP AG-6 efforts of "System Function Mapping to Levels of FORCEnet" spreadsheet provided by Professor Green.

THIS PAGE INTENTIONALLY LEFT BLANK

FORCEnet Level -1 - Today for Nations other than USA - may not be IP ready/applicable.
FORCEnet Level 0 - Full IT21 (level of USA Today)
FORCEnet Level 1 - Net Connected
FORCEnet Level 2 - Net Enabled
FORCEnet Level 3 - Fully Net Ready
FORCEnet Level 4 - Beyond FORCEnet

	System Function	Existing / Future System Stepping Stones					
		Level -1	Level 0	Level 1	Level 2	Level 3	Level 4
Systems	Messaging (text based)	Basic exchange server message handling system	Email and webservices	Email and webservices, multiple domain support	Email and webservices, gateway for translation of protocals and content, intrusion detection	Email and webservices with digital signatures and/or PKI, provide message content integrity, archive messages, interface with other government agencies and allies and non-government agencies, use mailguard, use profiler, intrusion detection, S/MIME	Email and webservices, digital signatures and/or PKI, guaranteed delivery, provide message content integrity, archive messages, interface with other government agencies and allies and non-government agencies, use mailguard, use profiler, intrusion detection, S/MIME
	Messaging (Multimedia / file / other data)	Email	Email and webservices	Email and webservices, multiple domain support	Email and webservices, gateway for translation of protocals and content, intrusion detection	Email and webservices with digital signatures and/or PKI, provide message content integrity, archive messages, interface with other government agencies and allies and non-government agencies, use mailguard, use profiler, intrusion detection, S/MIME	Email and webservices, digital signatures and/or PKI, guaranteed delivery, provide message content integrity, archive messages, interface with other government agencies and allies and non-government agencies, use mailguard, use profiler, intrusion detection, S/MIME
	Voice Comms (Analog/VOIP/Secure)	Airborne radio, Secure Phone	Software-reprogrammable, multi-band/multi-mode airborne radio, Secure Phone	VOIP Inc1, encryption	VOIP Inc2, increased voice quality, encryption, Disruption-Tolerant Networking, ability to access maps and video from other units and battlefield sensors, provide LOS and BLOS communication	VOIP Inc3, high voice quality, Disruption-Tolerant Networking, ability to access maps and video from other units and battlefield sensors, provide LOS and BLOS communication, operate as nodes in a network for mibile and fixed forces	High voice quality, Disruption-Tolerant Networking, ability to access maps and video from other units and battlefield sensors, provide LOS and BLOS communication, operate as nodes in a network for mibile and fixed forces
	Video/Picture Broadcast/Send - static data or local / ISR Realtime	Local video from Commercial Systems, Digital Cameras, military Camera systems in use, JPEG stills, disruption-tolerant networking	Local video from Commercial Systems, Digital Cameras, military Camera systems in use, JPEG stills, disruption-tolerant networking	Video from Commercial Systems, Digital Cameras, military Camera systems in use, JPEG stills, disruption-tolerant networking, secure	Real-time, Disruption-Tolerant Networking	Real-time, Disruption-Tolerant Networking	Real-time, Disruption-Tolerant Networking
	Tactical/Combat/Weapons Systems	Radar system capable of automatic detection and tracking of targets, integrated command and decision system, integrated weapons control system, integrated self defense system	Enhanced radar system capable of automatic detection and tracking of targets, integrated command and decision system, integrated weapons control system, integrated self defense system	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest, integrated with Ballistic Missile Defense Signal Processor like system, Remote Diagnostic capability	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest, integrated with Ballistic Missile Defense Signal Processor like system, provide real-time detection tracking and discrimination performance against targets representing ballistic-missile threats, Remote Diagnostic capability	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest, integrated with Ballistic Missile Defense Signal Processor like system, Remote Diagnostic capability
	Tactical Data Link	Netted communication and standard message format, high speed computer to computer digital radio communications	Netted communication and standard message format, high speed computer to computer digital radio communications	Jam resistant, improved security, increaded throughput, inceased granularity, secure voice	Beyond Line of Sight, no use of dedicated airborne relay, in-theater reachback capability,	Time Domain Multiple Access architecture standard, over extended ranges, automatic allocation of more capacity to units with the most traffic to transmit	Time Domain Multiple Access architecture standard, over extended ranges, automatic allocation of more capacity to units with the most traffic to transmit

Notional FORCEnet Capabilities

Systems	Command Support System	Global Command & Control Data Sharing System	Global Command & Control Data Sharing System	Improved Global Command & Control Data Sharing System	Enhanced Global Command & Control Data Sharing System	Enhanced Global Command & Control Data Sharing System	Enhanced Global Command & Control Data Sharing System
	Situational Awareness (operating picture compilation)	GCCS-M like system	GCCS-M like system	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest	Web enabled services in support of the Global Information Grid, reliable, decision quality information to bridge real-time and near real-time communities of interest
	Track DB Services	Track database management within GCCS-M like system, Track DB within systems	Track database management within GCCS-M like system, Track DB within systems	Track database management within GCCS-M like system, Track DB within systems	Improved track database management within GCCS-M like system, Track DB within systems	Enhanced track database management within GCCS-M like system, Track DB within systems	Enhanced track database management within GCCS-M like system, Track DB within systems
	Distributed Collaborative Planning Tools	VTC shore based, not on platforms	Chat, Whiteboard, email, IPWarChat and Sametime	Chat, Whiteboard, email, IPWarChat and Sametime	Video over IP	Full Multimedia Telepresence	Full Multimedia Telepresence
	Decision Aids	Stand alone	Data collaboration	Data collaboration and fusion	Information processing or simulating	Information processing or simulating to provide decision suggestions and predict enemies intent	Information processing or simulating to provide decision suggestions and predict enemies intent
	Network Classification Security - Coalition / OGD / Multi-level / Caveat	Manually downgrade, automized sanitation	Manually downgrade, automized sanitation	High assurance internet protocol encrytor	Improved high assurance internet protocol encrytor, Content Based Encryption, Joint Cross Domain eXchange, protection level 4	Content Based information security, integration of JCDX into Service Oriented Architecture, labeling service for assigning security level and provide signature for verification	Content Based information security, integration of JCDX into Service Oriented Architecture, labeling service for assigning security level and provide signature for verification
	Comms Bearers Bandwidths	Increase bandwidth load	Increased Satcom Bandwidth	Increase in overall number of sensors increases bandwidth use	Better data fusion and asset allocation decreases bandwidth congestion	Increase in number of sensors and connectivity increases bandwidth usage, increase in data being transferred and detail of data increases bandwidth needs	Bandwidth allocation solutions necessary to deliver true NCO capability
	IP Communication Bearers	IPv4, Satelite, wideband and reachback	Improved wideband gapfiller system, wideband and reachback, multifunction information distribution system-low volume terminal	Improved wideband gapfiller system, wideband and reachback, multifunction information distribution system-low volume terminal, LOS WAN	IPv6, LOS WAN with use of geosynchronous satellites to provide worldwide, secure, survivable, protected communications	Capability to provide multiband, multimedia, and worldwide reach-back	Capability to provide multiband, multimedia, and worldwide reach-back, integrate with wideband gapfiller system
	Networks	Coalition Network Centric Capability	Coalition Network Centric Capability	Coalition Network Centric Capability	Improved Coalition Network Centric Capability	Enhanced Coalition Network Centric Capability	Enhanced Coalition Network Centric Capability
	Network Management Services	Network Services	Dynamic Data Link Network Management	Dynamic Data Link Network Management	Capability to provide multiband, multimedia, and worldwide reach-back	Capability to provide multiband, multimedia, and worldwide reach-back	Capability to provide multiband, multimedia, and worldwide reach-back
	Information Manager	Bandwidth Managers	Bandwidth Managers	Bandwidth Managers	Bandwidth Managers	Automated Network Control Center	Automated Network Control Center
	Data Sharing	Sharing via translators with latency	Sharing via translators	Sharing via translators	Sharing via improved translators, National Collaborative Capability	Sharing via enhanced translators, International Collaborative Capability	Sharing via enhanced translators, International Collaborative Capability
	Network Reach into other nodes	ISR / C2	Improved ISR / C2	Remote Monitoring, Remote Diagnostics, Weapons Data Link	Remote Monitoring, Remote Diagnostics, Weapons Data Link	Remote Monitoring, Remote Diagnostics, Weapons Data Link	Remote Monitoring, Remote Diagnostics, Weapons Data Link, Autonomic Control
	Information Fusion	Very limited capability	Network Centric Collaborative Targeting	Low Speed, Limited Data Integration for Information, COP	Data Integration for Information, COP, CTP	High Speed Data Integration for Information, COP, CTP, FCP	High Speed Data Integration for Informatio, COP, CTP, FCP, Remotely Accessable

Notional FORCEnet Capabilities

APPENDIX C: PRELIMINARY MODELING ANALYSIS FOR VIGNETTES 1, 2, 4, 5, AND 8

THIS PAGE INTENTIONALLY LEFT BLANK

Vignette 1 – Training & Planning as the Coalition ESG force 'gels' together during the transit and assembly Vignette (D+0)

A. Coalition Force ESG conducts starts planning, organizing and assembling the Coalition Force.

B. Goals of Coalition Force ESG are:

(1) Good level of understanding of commander's intent

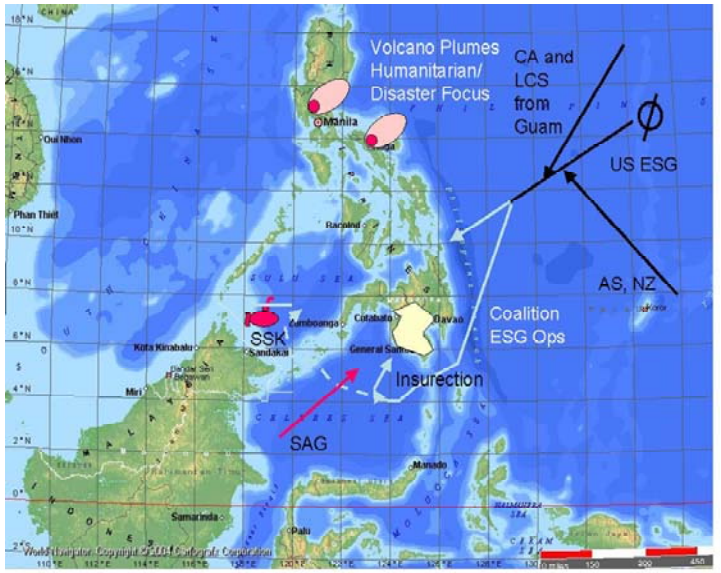
(2) Coalition Forces are tailored to the applicable operation

(3) All platforms are established on a common network

(4) Mission, Contingency and branch plans are developed and distributed to all applicable C2 nodes within the ESG

(5) High Value Units are recognized and are allocated with mission priority for Force Protection

(6) An immediate and accurate status picture of all ESG platforms is available to all units (I.e, identification, equipment status, location, mission status,…etc.)



Vignette Assumptions:

•DOTMLFP analysis only required for this Vignette
•Commander's intent is captured in C2 node databases and distributed to other C2 nodes
•ESG initiates Commander's Guidance for all U.S and attached coalition assets
•All equipment (weapons, sensors, C2 system) are operational on all platforms with required fuel and full ammunition loads (missiles, munitions, small caliber rounds).

Vignette 2 - A littoral transit phase against a FIAC threat (D+1)

A. FIAC threat postured to attack from close to Mindanao (initially concealed in coastal traffic) or from close to Sarangani or Balut Islands (concealed within the islands). FIAC threat consist of: (5 to 20) Type 1 FIAC (armed with RPG/large blast bomb – range 500m) or (2 to 5) Type 2 FIAC (armed with multiple launch rockets – range 8km)

B. Coalition Force ESG conducts transit through Sarangani Strait while locating and destroying the FIAC threat within the littoral environment. The ESG conducts this operation with the following:
3 X LCS, 2 X DDG, 2 X Coalition FFG/DDG, 1 X MPA/AWACS/UAV/HELO
guarding HVU
1 X LHD, 1 X LPD, 7 X NGO vessels

C. Goals of the Coalition Force ESG are:
(1) Minimize detect-to-kill time for engagements

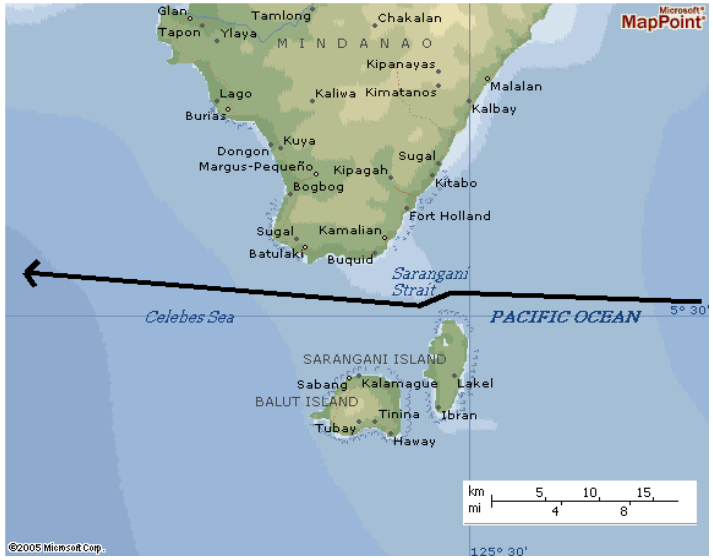
(2) Allow no leakers

(3) Successfully intercept any leakers

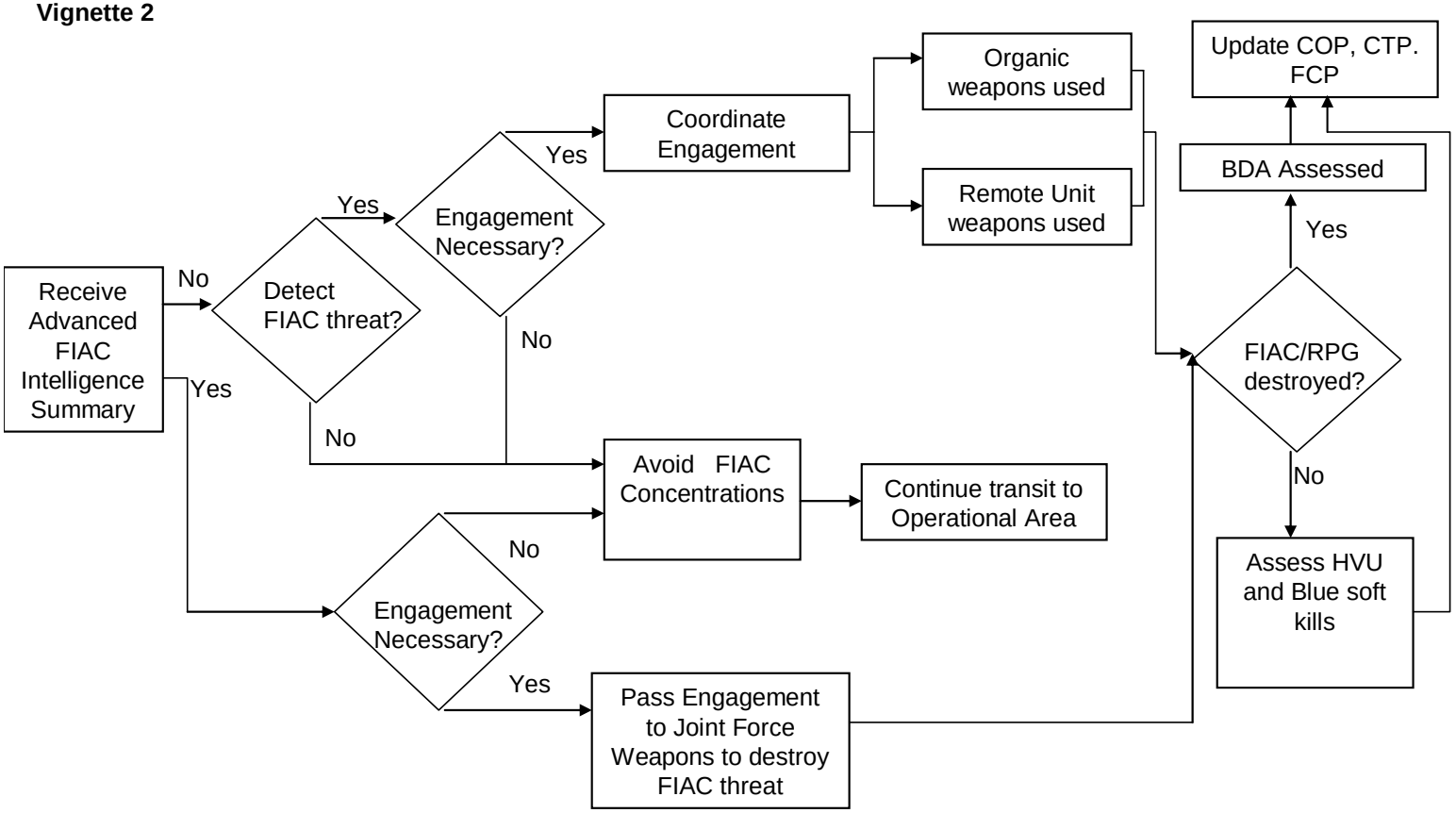
(4) Minimize number of HVU soft-kills

(5) Minimize number of Blue combatant craft soft-kills

(6) Broadcast FIAC contacts to other ESG platforms in timely manner



Vignette 2



Vignette Assumptions:

- Coalition ESG can safely maneuver from FIAC threat if locations are known
- FIAC threat can only cause soft kills to friendly Blue assets (HVU's included)
- Utilization of Joint Assets are available for early shaping of battlespace if FIAC threat detected early
- Enhanced FORCEnet levels facilitate early intelligence summaries in advance
- ESG platforms will encounter at most three FIACs each

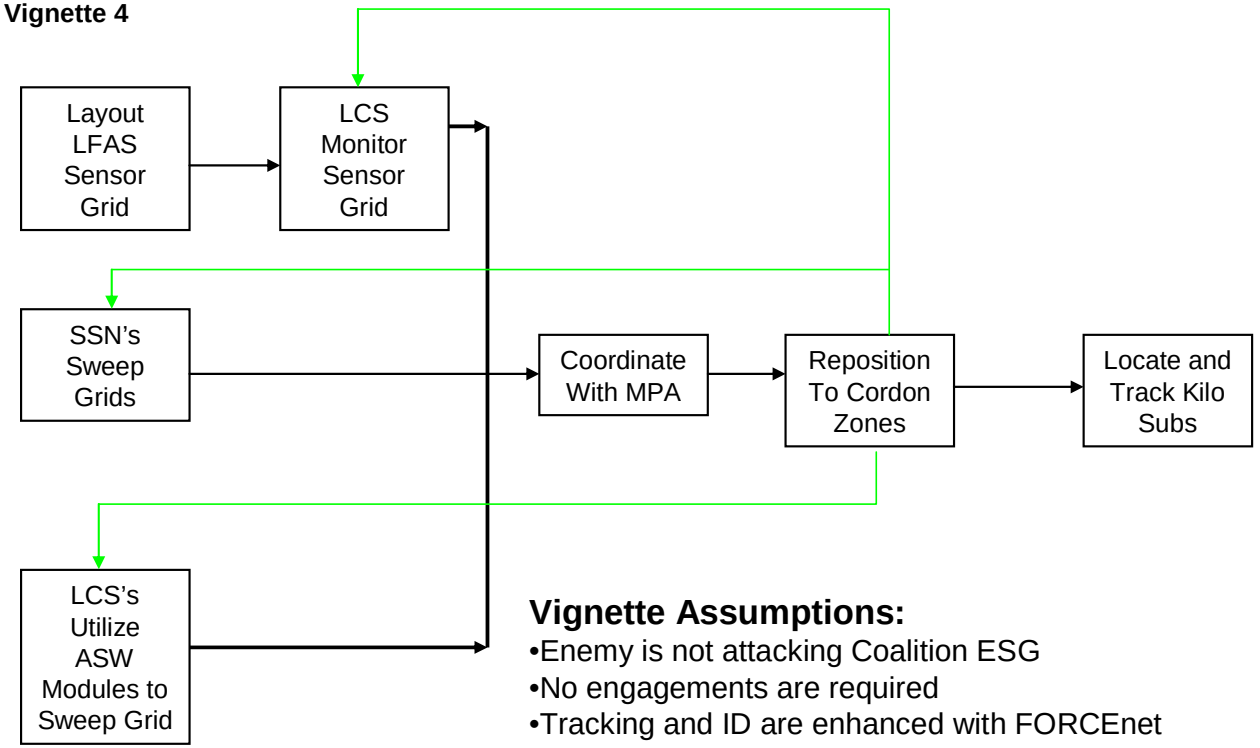
Vignette 4 ASW against the Kilo threat (D+3)

A. ESG has passed through Sulu Archipelogo into the Sulu Sea. Must locate two enemy Kilo submarines.

B. Coalition Force locates enemy submarines with
1 X MPA, 2 X SSN, 3 X LCS with LFAS and barrier sensors,

C. Goals of Coalition Force ESG are:
(1) Locate and classify all enemy submarines in a timely manner

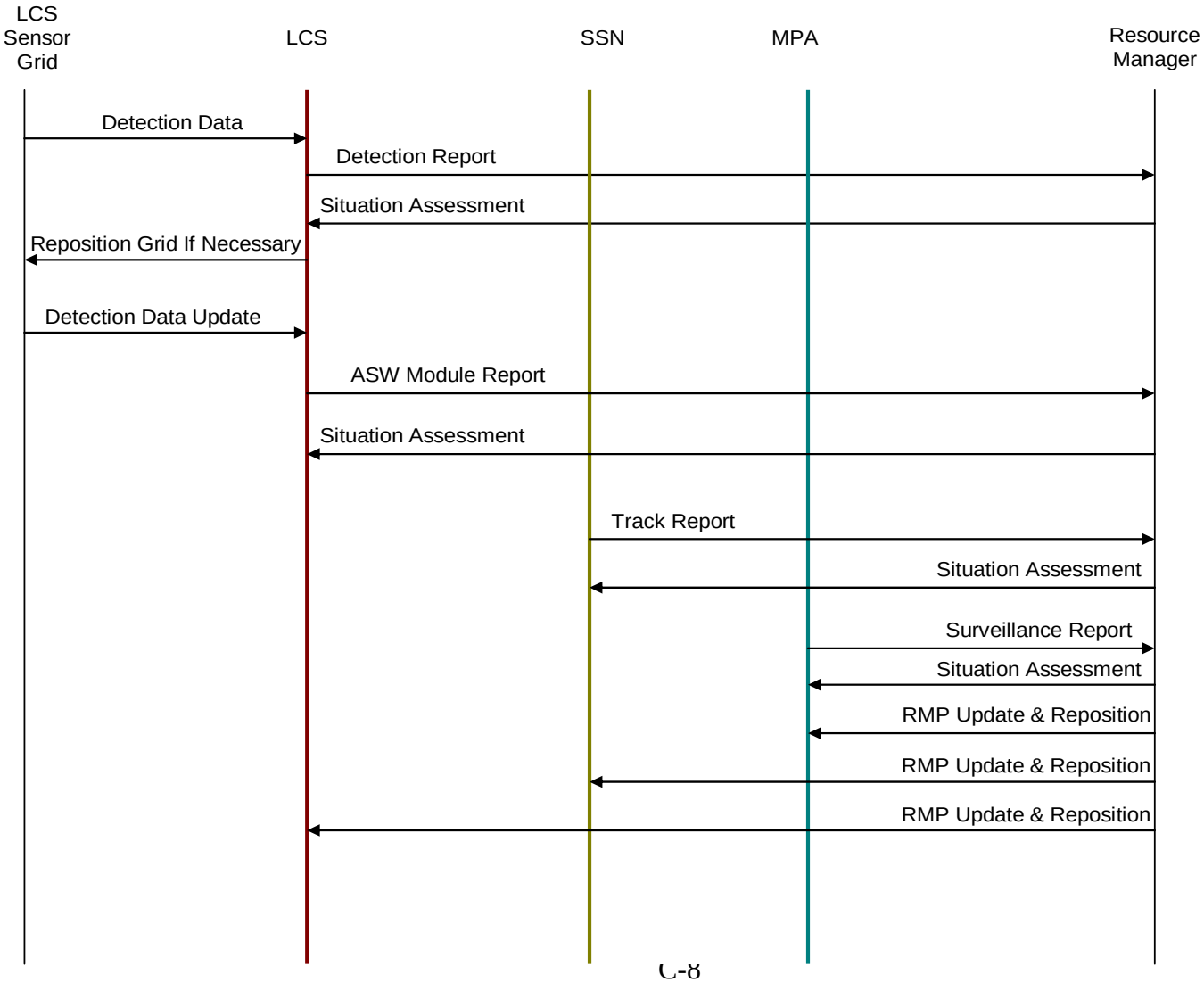
Vignette 4



Vignette Assumptions:

•Enemy is not attacking Coalition ESG
•No engagements are required
•Tracking and ID are enhanced with FORCEnet
•LCS equipped with ASW module are assigned to localising missions
•The LFAS barriers will relay the detections (if any) via RF transmitter to the LCS
•Using the LCS's helo as a relay and to lay the LFAS barriers, the helo will drop a string of LFAS about 30 nm
away from the LCS, this keeps the submarine and its weapons out of range of the LCS, and maximizes
the on-station time of the helo.
•The MPA can be used in lieu of LCS helos ifnecessary to provide relay for LFAS barrier monitoring

Vignette 4


LCS Sensor Grid
LCS
SSN
MPA
Resource Manager
Detection Data
Detection Report
Situation Assessment
Reposition Grid If Necessary
Detection Data Update
ASW Module Report
Situation Assessment
Track Report
Situation Assessment
Surveillance Report
Situation Assessment
RMP Update & Reposition
RMP Update & Reposition
RMP Update & Reposition

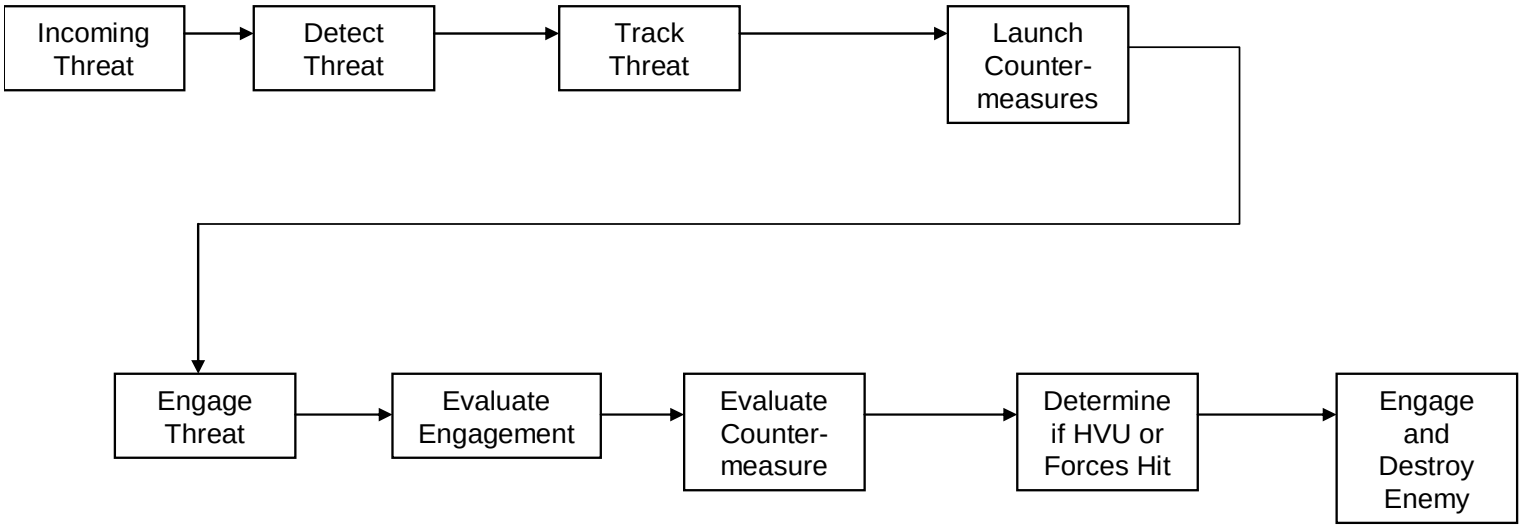
Vignette 5 - AAW and/or ASMD should the Indonesian forces achieve launch position against ESG (D+8)

A. While Coalition Force is searching for Kilo submarines enemy launches missile attack on Coalition Forces. Enemy units are
(2) Parchim Corvette, 3 Van Spijk FFG, (2) Kilo Submarines

B. Coalition Force must defend HVU with
(3) LCS, (2) DDG, (1) EC-2C, (2) Coalition FFG/DDG
HVU
(1) LHD/CVN, (1) LPD

C. Goals of Coalition Force ESG are:
(1) Minimize detect-to-kill time for engagements
(2) Maximize size of supportable engagement envelope
(3) Allow no leakers
(4) Successfully intercept any leakers
(5) Minimize number of HVU soft-killed
(6) Minimize number of Blue combatant craft soft-killed
(7) Broadcast enemy contacts to other ESG platforms in a timely manner

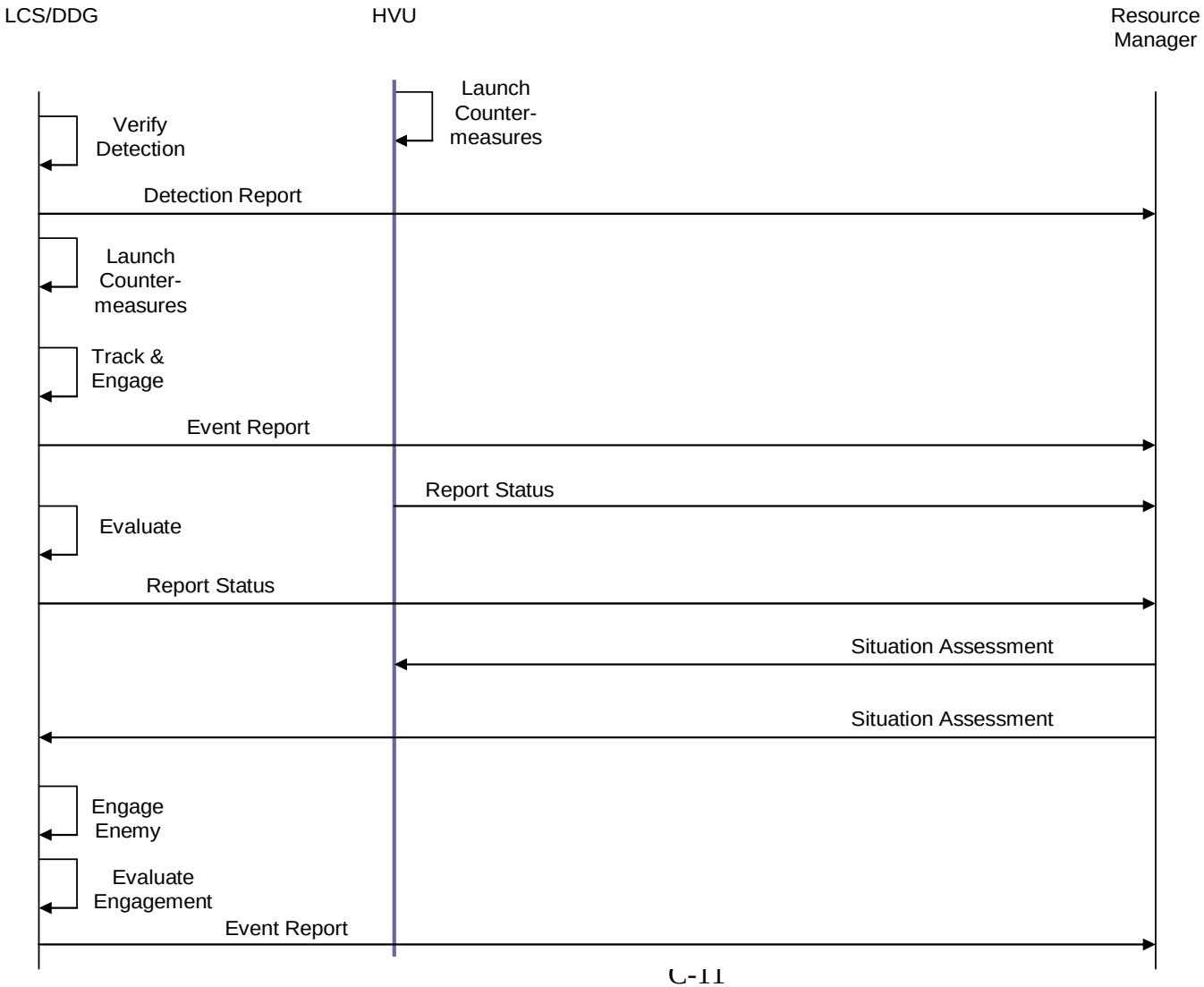
Vignette 5



Vignette Assumptions:

•ESG platforms will encounter at most three air/missile attacks each
•FORCEnet provides early and accurate tracking of air/missile threat
•

Vignette 5


LCS/DDG
HVU
Resource Manager
Launch Counter-measures
Verify Detection
Detection Report
Launch Counter-measures
Track & Engage
Event Report
Report Status
Evaluate
Report Status
Situation Assessment
Situation Assessment
Engage Enemy
Evaluate Engagement
Event Report

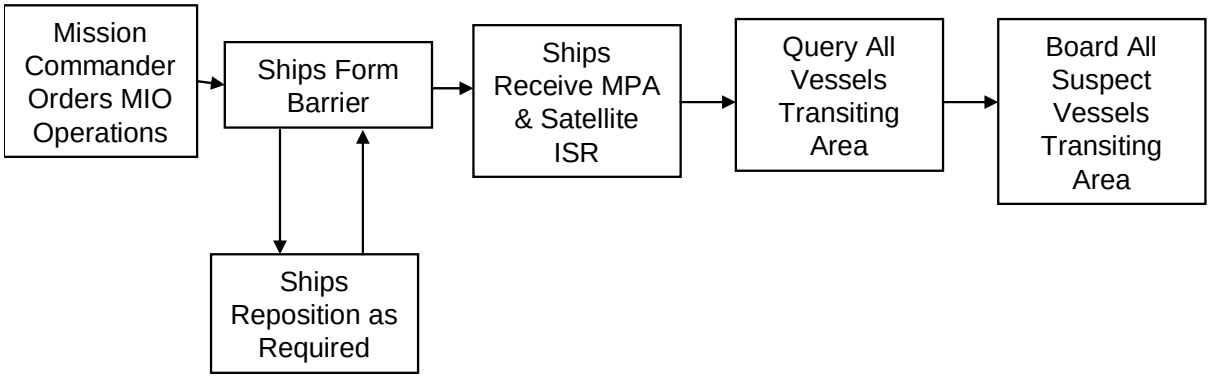
Vignette 8 – MIO, to stop Indonesia reinforcing the insurgents ashore, by sea (D+11)

A. Coalition Force ESG set up an MIO barrier to prevent troop and supply reinforcements to insurgents. Enemy forces conducting the reinforcement missions will utilize the following means: Up to 50 fishing boats, 10 X small craft/coastal traders, and 4 X large merchants.

B. Coalition Force ESG that query and conduct searches at the barrier include:
2 X DDG, 3 X LCS, 2 X Coalition FFG/DDG, 2 X RHIBs and boarding parties available per vessel, and MPA/AWACS/UAV/helos

C. Goals of Coalition Force ESG are:
(1) Locate, identify, stop, and search all enemy vessels with insurgent reinforcement personnel and supplies
(2) Minimize number of incorrectly identified craft boarded
(3) Minimize time taken to inspect each vehicle

Vignette 8



Initial Queries Should Include:

- What is your vessels name?
- What is the registry and flag of your vessel ?
- What was your last port of call?
- What is your cargo?

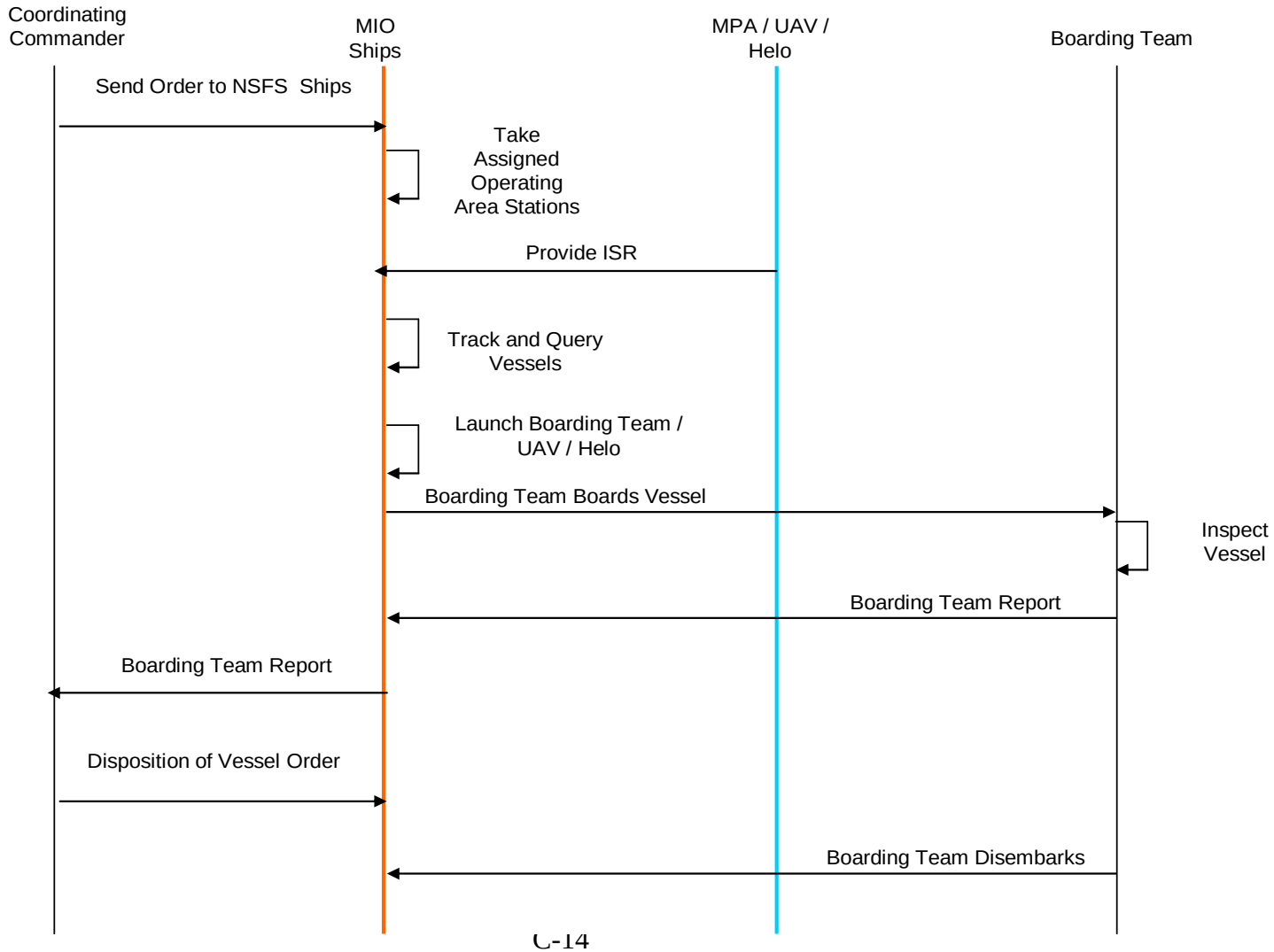
Suspect Vessels are declared a Critical Contacts of Interest (CCOI). CCOI's are any vessel -

- Transiting towards the Phillipines
- Who's name is registered under an Indonesian Owner or National Flag
- Who's last port of call was in Indonesia
- Who's cargo is questionable

Vignette Assumptions:

•Enemy is not attacking Coalition ESG
•No engagements are required
•Tracking and ID are enhanced with FORCEnet
•Unmarked civilian vessels are arriving from a localised direction such that ESG can effectively perform MIO
•The 50 small fising boats will travel in groups of fives
•The 10 small craft/coastal traders travel in groups of twos
•The 4 large merchants will travel individually

Vignette 8


Coordinating Commander
MIO Ships
MPA / UAV / Helo
Boarding Team
Send Order to NSFS Ships
Take Assigned Operating Area Stations
Provide ISR
Track and Query Vessels
Launch Boarding Team / UAV / Helo
Boarding Team Boards Vessel
Inspect Vessel
Boarding Team Report
Boarding Team Report
Disposition of Vessel Order
Boarding Team Disembarks

APPENDIX D: COALITION FORCENET ECONOMIC COST MODELS

THIS PAGE INTENTIONALLY LEFT BLANK

Assume all payments are made at the end of fiscal year
20-year LCC model (in million dollars) **3.00%**

FY	Year		PROCUREMENT	ANNUAL OPS & SUP	Total Cost	End of year factor	Present value	Present Value Procurement	Present Value O&S Cost
2005	0				$ -	1.00	$ -	$ -	$ -
2006	1		$ 3.20		$ 3.20	0.97	$ 3.11	$ 3.11	$3.11
2007	2			$ -	$ -	0.94	$ -	$ -	$0.79
2008	3			$ -	$ -	0.92	$ -	$ -	$0.78
2009	4			$ -	$ -	0.89	$ -	$ -	$0.76
2010	5			$ -	$ -	0.86	$ -	$ -	$0.75
2011	6			$ -	$ -	0.84	$ -	$ -	$0.73
2012	7			$ -	$ -	0.81	$ -	$ -	$0.72
2013	8			$ -	$ -	0.79	$ -	$ -	$0.70
2014	9			$ -	$ -	0.77	$ -	$ -	$0.70
2015	10			$ -	$ -	0.74	$ -	$ -	$0.68
2016	11			$ -	$ -	0.72	$ -	$ -	$0.67
2017	12			$ -	$ -	0.70	$ -	$ -	$0.66
2018	13			$ -	$ -	0.68	$ -	$ -	$0.64
2019	14			$ -	$ -	0.66	$ -	$ -	$0.63
2020	15			$ -	$ -	0.64	$ -	$ -	$0.62
2021	16			$ -	$ -	0.62	$ -	$ -	$0.61
2022	17			$ -	$ -	0.61	$ -	$ -	$0.60
2023	18			$ -	$ -	0.59	$ -	$ -	$0.58
2024	19			$ -	$ -	0.57	$ -	$ -	$0.57
2025	20			$ -	$ -	0.55	$ -	$ -	$0.56
Total			**$ 3.20**	**$ -**	**$ 3.20**		**$ 3.11**	$ 3.11	$15.86

Total LCC Discounted cost per ship (millions $): **$ 3.11**

Spiral #1 (FY2006-2009) Command and Control: CENTRIXS units for each unit within the coalition force (IP based)
PROCUREMENT Cost of obtaining the system, Installation Cost, Initial Training Cost, Initial Spares and Logistics Cost
RESEARCH & DEVELOPMENT COST INCLUDES: Cost of designing the prototype that lead up to the first working system
ANNUAL OPERATION & SUPPORT COST INCLUDE System Integration cost, Maintenance Cost, and Repair Cost

Figure D.1. FORCEnet Level 1 LCC

Assume all payments are made at the end of fiscal year
20-year LCC model (in million dollars) **3.00%**

FY	Year	PROCUREMENT	ANNUAL OPS & SUP	Total Cost	End of year factor	Present value	Present Value Procurement	Present Value O&S Cost
2005	0			$ -	1	$ -	$ -	$ -
2006	1	$ 3.20		$ 3.20	0.971	$ 3.11	$ 3.11	$ -
2007	2		$ -	$ -	0.943	$ -	$ -	$0.79
2008	3		$ -	$ -	0.915	$ -	$ -	$0.78
2009	4		$ -	$ -	0.888	$ -	$ -	$0.76
2010	5	$ 5.90	$ -	$ 5.90	0.863	$ 5.09	$ 5.09	$0.75
2011	6		$ -	$ -	0.837	$ -	$ -	$1.74
2012	7		$ -	$ -	0.813	$ -	$ -	$1.70
2013	8		$ -	$ -	0.789	$ -	$ -	$1.67
2014	9		$ -	$ -	0.766	$ -	$ -	$1.65
2015	10		$ -	$ -	0.744	$ -	$ -	$1.62
2016	11		$ -	$ -	0.722	$ -	$ -	$1.59
2017	12		$ -	$ -	0.701	$ -	$ -	$1.56
2018	13		$ -	$ -	0.681	$ -	$ -	$1.53
2019	14		$ -	$ -	0.661	$ -	$ -	$1.50
2020	15		$ -	$ -	0.642	$ -	$ -	$1.47
2021	16		$ -	$ -	0.623	$ -	$ -	$1.44
2022	17		$ -	$ -	0.605	$ -	$ -	$1.41
2023	18		$ -	$ -	0.587	$ -	$ -	$1.39
2024	19		$ -	$ -	0.570	$ -	$ -	$1.36
2025	20		$ -	$ -	0.554	$ -	$ -	$1.33
Total		**$ 9.10**	**$ -**	**$ 9.10**		**$ 8.20**	8.20	$26.05

Total LCC Discounted cost per ship (in million dollars): $ 8.20

Spiral #1 (FY2006-2009) Command and Control: CENTRIXS units for each unit within the coalition force (IP based)
Spiral #2 (FY2010-2014) Tactical Data Link: Link 22 capability for each unit within the coalition force (highly
PROCUREMEN Cost of obtaining the system, Installation Cost, Initial Training Cost, Initial Spares and Logistics Cost
RESEARCH & DEVELOPMENT COST INCLUDES Cost of designing the prototype that lead up to the first working system
ANNUAL OPERATION & SUPPORT COST INCLU System Integration cost, Maintenance Cost, and Repair Cost

Figure D.2. FORCEnet Level 2 LCC

Assume all payments are made at the end of fiscal year
20-year LCC model (in million dollars) **3.00%**

FY	Year	PROCUREMENT	ANNUAL OPS & SUP	Total Cost	End of year factor	Present value	Present Value Procurement	Present Value O&S Cost
2005	0			$ -	1.00	$ -	$ -	$ -
2006	1	$ 3.20		$ 3.20	0.97	$ 3.11	$ 3.11	$ -
2007	2		$ -	$ -	0.94	$ -	$ -	$0.79
2008	3		$ -	$ -	0.92	$ -	$ -	$0.78
2009	4		$ -	$ -	0.89	$ -	$ -	$0.76
2010	5	$ 5.90	$ -	$ 5.90	0.86	$ 5.09	$ 5.09	$0.75
2011	6		$ -	$ -	0.84	$ -	$ -	$1.74
2012	7		$ -	$ -	0.81	$ -	$ -	$1.70
2013	8		$ -	$ -	0.79	$ -	$ -	$1.67
2014	9	$ 16.80	$ -	$ 16.80	0.77	$ 12.88	$ 12.88	$1.65
2015	10		$ -	$ -	0.74	$ -	$ -	$2.96
2016	11		$ -	$ -	0.72	$ -	$ -	$2.90
2017	12		$ -	$ -	0.70	$ -	$ -	$2.85
2018	13		$ -	$ -	0.68	$ -	$ -	$2.79
2019	14		$ -	$ -	0.66	$ -	$ -	$2.74
2020	15		$ -	$ -	0.64	$ -	$ -	$2.68
2021	16		$ -	$ -	0.62	$ -	$ -	$2.63
2022	17		$ -	$ -	0.61	$ -	$ -	$2.58
2023	18		$ -	$ -	0.59	$ -	$ -	$2.53
2024	19		$ -	$ -	0.57	$ -	$ -	$2.48
2025	20		$ -	$ -	0.55	$ -	$ -	$2.43
Total		**25.90**	**0.00**	**$ 25.90**		**$ 21.07**	$ 21.07	$39.43

Total LCC Discounted cost per ship (millions $): $ 21.07

Spiral #1 (FY2006-2009) Command and Control: CENTRIXS units for each unit within the coalition force (IP based)
Spiral #2 (FY2010-2014) Tactical Data Link: Link 22 capability for each unit within the coalition force (highly enhanced TADIL)
Spiral #3 (FY2014-2018) CEC-like capability, Enhanced networks and connectivity into combat systems, weapons and

PROCUREMENT COST Cost of obtaining the system, Installation Cost, Initial Training Cost, Initial Spares and Logistics Cost
RESEARCH & DEVELOPMENT COST INCLUDES: Cost of designing the prototype that lead up to the first working system
ANNUAL OPERATION & SUPPORT COST INCLUDES: System Integration cost, Maintenance Cost, and Repair Cost

Figure D.3. FORCEnet Level 4 LCC

						(in FY2006 $)
			Cost (M)	PV factor	PV Cost (M)	
Spiral 1	Procurement	System Integration Cost	$ 2.00	0.97	$ 1.94	
	(Year 2006)	Software	$ 0.05	0.97	$ 0.05	
		Hardware	$ 0.50	0.97	$ 0.49	
		Admin and Logistics Cost	$ 0.10	0.97	$ 0.10	
		Installation	$ 0.40	0.97	$ 0.39	
		Initial Training	$ 0.01	0.97	$ 0.01	
		Initial Spares	$ 0.14	0.97	$ 0.14	
	Total		$ 3.20		$ 3.10	
Spiral 2	Procurement	System Integration Cost	$ 3.40	0.97	$ 3.30	
	(Year 2010)	Software	$ 0.40	0.97	$ 0.39	
		Hardware	$ 0.70	0.97	$ 0.68	
		Admin and Logistics Cost	$ 0.20	0.97	$ 0.19	
		Installation	$ 1.00	0.97	$ 0.97	
		Initial Training	$ 0.05	0.97	$ 0.05	
		Initial Spares	$ 0.15	0.97	$ 0.15	
	Total		$ 5.90		$ 5.72	
Spiral 3	Procurement	System Integration Cost	$ 9.60	0.97	$ 9.31	
	(Year 2014)	Software	$ 1.00	0.97	$ 0.97	
		Hardware	$ 3.30	0.97	$ 3.20	
		Admin and Logistics Cost	$ 0.50	0.97	$ 0.49	
		Installation	$ 1.60	0.97	$ 1.55	
		Initial Training	$ 0.20	0.97	$ 0.19	
		Initial Spares	$ 0.60	0.97	$ 0.58	
	Total		$ 16.80		$ 16.30	
Spiral 1	O&S Cost (20 year LCC)	From Year 2006 to Year 2025			$ 15.86	
Spiral 2	O&S Cost (20 year LCC)	From Year 2010 to Year 2025			$ 10.19	
Spiral 3	O&S Cost (20 year LCC)	From Year 2014 to Year 2025			$ 13.38	
Fn Level I	O&S Cost (20 year LCC)	From Year 2006 to Year 2025			$ 15.86	
Fn Level II	O&S Cost (20 year LCC)	From Year 2006 to Year 2025 Add O&S for Spiral I&II for corresponding years			$ 26.05	
Fn Level IV	O&S Cost (20 year LCC)	From Year 2006 to Year 2025 Add O&S for Spiral I, II, & IV for corresponding years			$ 39.43	

Figure D.4. LCC Summary Data for FORCEnet Levels I, II, and IV

APPENDIX E: ACRONYM LIST

THIS PAGE INTENTIONALLY LEFT BLANK

Acronym	Definition
AAW	Anti-Air Warfare
AB	Alpha Bravo, Officer in Charge
ABM	Agent Based Modeling
ABMA	Automated Battle Management Aids
AG-1	Action Group 1
AG-6	Action Group 6
AM	Alpha Mike, Maritime Interdiction Warfare Commander
ANZAC	Frigate Class Ship, Australia
AS	Alpha Sierra, Surface Warfare Commander
ASCM	Anti-Ship Cruise Missile
ASG	Abu-Sayyaf Group
ASMD	Anti-Ship Missile Defense
ASuW	Anti-Surface Warfare
ASW	Anti-Submarine Warfare
ATM	Asynchronous Transfer Mode
AW	Alpha Whiskey, Air Warfare Commander
AWACS	Airborne Warning and Control System
AWD	Air Warfare Destroyer, United Kingdom
AX	Alpha X-ray, Sub-surface Warfare Commander
BDA	Battle/ Bomb Damage Assessment
C2	Command and Control
C4I	Command, Control, Computers, Communication, Intelligence, Surveillance, and Reconnaissance
C5I	Command, Control, Communications, Computers, Combat Direction, and Intelligence
CCOI	Critical Contacts of Interest
CDD	Capabilities Development Document
CDS	Cross Domain Solutions
CEC	Cooperative Engagement Capability
CENTRIXS	Combined Enterprise Regional Information Exchange System
CESG	Coalition Expeditionary Strike Group
CFF	Call For Fire
CFMCC	Combined Forces Maritime Component Commander
CG	Cruiser Class Ship, United States
COA	Course of Action
COE	Common Operating Environment
COMS	Communications
CONET	Coalition Network
COP	Common Operational Picture
COTS	Commercial Off-The Shelf
CTF	Coalition Task Force

Acronym	Definition
CTP	Common Tactical Picture
CWSP	Commercial Wideband Satellite Communication Program
DDG	Destroyer Class Ship, United States
DIA	Defense Intelligence Agency
DMA	Defense Mapping Agency
DOTMLPF	Doctrine, Organization, Training, Materiel, Leadership, Personnel, and Facilities
E-2C	Air Surveillance and Patrol Aircraft, United States
EHF	Extremely High Frequency (30 – 300 GHZ)
ERGM	Extended Range Guided Munition
ESG	Expeditionary Strike Group
FCP	Fire Control Picture
FFG	Frigate Class Ship, United States
FFH	Frigate Class Ship, Australia & New Zealand
FIAC	Fast Inshore Attack Craft
Fn	FORCEnet
FOC	Full Operational Capability
FY	Fiscal Year
GAM	Free Aceh Movement in Aceh, Indonesia
GBS	Global Broadcast Services
GPS	Global Positioning System
HA-DR	Humanitarian Aid and Disaster Relief
HCI	Human-Centric Integration
HF	High Frequency (3 to 30 MHz)
HVU	High Value Units (LSD, LPD, LHD)
ICD	Initial Capabilities Document
IFF	Identification Friend or Foe
INMARSAT	International Marine/ Maritime Satellite
IO	Information Operations
IOC	Initial Operational Capability
IP	Internet Protocol
IPR	In Progress Review
IR	Infrared
ISR	Intelligence, Surveillance and Reconnaissance
IT-21	Information Technology for the 21st Century (United States Navy Program)
JI	Jermaah Islamiyah
JREAP	Joint Range Extension Application Protocol
JTRS	Joint Tactical Radio System
JWICS	Joint Worldwide Intelligence Communications System
KH-35	High Speed Type Missiles
KPP	Key Performance Parameters
LCC	Life Cycle Cost
LCS	Littoral Combat Ship, United States

Acronym	Definition
LFAS	Low-Frequency-Active Sonar
LHD	Large Amphibious Ship, United States
LPD	Large Amphibious Ship, United States
LRLAP	Long Range Land Attack Projectile
LSD	Large Amphibious Ship, United States
LST	Transport Ship for Troops, Vehicles and Supplies
M2M	Machine to Machine
MAR	Maritime Systems
MDR	Metadata Repository
MILF	Moro Islamic Liberation Front
MIO	Maritime Interdiction Operations
MLS	Multi-Level Security
MOE	Measures of Effectiveness
MOP	Measures of Performance
MPA	Maritime Patrol Aircraft
MRV	Multi-Role Vehicle, United Kingdom
MSSE	Master of Science in Systems Engineering
NATO	North Atlantic Treaty Organization
NCCT	Network-Centric Collaborative Targeting
NCW	Network-Centric Warfare
NFCS	Naval Fires Control System
NGO	Non-Governmental Organization
NH-90	Military Helicopter, Australia
NILE	NATO Improved Link Eleven
NOC	National Operations Center
NPS	Naval Postgraduate School
NSWC	Naval Surface Warfare Center
NWP	Naval Warfare Publication
OA	Open Architecture
O & S	Operations and Support
OMB	Office of Management and Budget, United States Government
ONI	Office of Naval Intelligence
OODA	Observe, Orient, Decide, Act
OOTW	Operations Other Than War
Op	Operational
OV	Operational View
P3-K	Maritime Patrol Aircraft, New Zealand
PHD	Port Hueneme Division
PSK-M	Modern Fast Patrol Boat
PV	Present Value
QoS	Quality of Service
R & D	Research and Development
RDML	Rear Admiral
RDT&E	Research, Development, Test & Evaluation
RF	Radio Frequency

Acronym	Definition
RF	Radio Frequency
RHIB	Rigid Hull Inflatable Boat
RMP	Recognized Maritime Picture
ROE	Rules of Engagement
RPG	Rocket Propelled Grenade
S2C	Speed to Capability
SACC-A	Supporting Arms Coordination Center Activity
SAG	Surface Action Group
SH-2G	Military Helicopter, Australia & New Zealand
SHF	Super High Frequency (3-30 GHz)
SIAP	Single Integrated Air Picture
SONET	Synchronous Optical Network
SOW	Statement of Work
SSL	Secure Socket Layer
SSN	Nuclear-powered Attack Submarine (Virginia Class, United States)
STK	Satellite Tool Kit
SV	Systems View
TACC	Tactical Air Control Center
TADIL	Tactical Digital Information Link
TDMA	Time Division Multiple Access
TEWA	Threat Evaluation and Weapon Assignment
TOF	Time of Flight
TTCP	The Technical Cooperation Program
TTPs	Tactics, Techniques, and Procedures
UAV	Unmanned Aerial Vehicle
UHF	Ultra-high Frequency (300 to 3000 MHz)
USN	United States Navy
VOIP	Voice Over Internet Protocol

LIST OF REFERENCES

ALRI - Navy of the Republic of Indonesia, Global Security Website, April 2005. http://www.globalsecurity.org/military/world/indonesia/alri.htm

Australian Government Department of Defense, "*NCW Roadmap,"* Chapter 8, October 2005.

Chamberlain, Sam (Ph.D.) "*The Formal Representation of Administrative and Operational Relationships within Defense Organizational Constructs*," presented at the CCRTS 2006, San Diego, California.

Cohort #3, "*FORCEnet Implications for a Coalition Maritime Force*," Capstone Project, Naval Postgraduate School, Monterey, California, 2005.

Clark, Vern, Admiral UASN, Chief of Naval Operations and Michael W. Hagee, General USMC, Commandant of the Marine Corp, *"FORCEnet A Functional Concept for the 21st Century."* http://enterprise.spawar.navy.mil/body.cfm?Topic_ID=1280&Type=R&category=23%20%20%20%20%20%20%20%20&subcat=45

CJCSI 3010.02 Series, "*Joint Future Concepts Process*."

CJCSI 3170.01E, "*Joint Capabilities Integration and Development System,"* 11 May 2005.

CJCSI 6212, *"Interoperability and Supportability of Information Technology and National Security Systems,"* 8 March 2006

Command, Control, Communication and Computer Intelligence Reconnaissance (C4ISR), RADM Mark R. Milliken, Director, Navy International Program Office, May 18, 2004.

DoD Architecture Framework Working Group, "*DOD Architecture Framework," Version 1.0, "Definitions and Guidelines,"* February 2004.

DoD, *Defense Acquisition Guidebook, Version 1.0*, October 2004.

DoD, Directive 8320.2, *"Data Sharing in a Net-Centric Department of Defense,"* December 2004. http://www.dtic.mil/whs/directives/corres/pdf/d83202_120204/d83202p.pdf

DoD, Office of Force Transformation, *" The Implementation of Network-Centric Warfare,"* January 2005. http://www.oft.osd.mil/library/library_files/document_387_NCW_Book_LowRes.pdf

DODD 4630.5, *"Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),"* May 2004.

DODD, 5000.1, *"The Defense Acquisition System,"* May 2003.

DoD, *"Quadrennial Defense Review Report,"* February 2006.

FORCEnet Architecture and Standards Volume 1 & 2, Office of the Chief Engineer, SPAWAR 05, 30 April 2004

Geocities website,*"Parchim-I' Class Anti-Submarine Frigates Projekt 133.1,"* September 2006. http://www.geocities.com/~uwezi/ships/parchim.html
http://en.wikipedia.org/wiki/Kilo_class_submarine

Green, Mike SI3123 briefing (Network Centric Architectures), Naval Postgraduate School, January 2006

Kelton, W. David , Randall. P. Sadowski, and David. T. Sturrock, *Simulation with Arena*, 3rd edition, McGrall-Hill.

Lawlor, Maryann, *Delay Ignites Frustration*, Signal Magazine, July 2006, http://www.afcea.org/signal/articles

Martinez, Carlos E., Kenneth L. Mullins, and Karl S. Sullivan, *Naval Warfare Publication NWP 3-56*, Navy Warfare Development Command, 2004

Miller, Dr Janet E., *"Participatory Design Methods for Command and Control Systems,"* Air Force Research Laboratory/HECS, 2006.

Morris, Edwin , Linda Levine, Craig Meyers, Pat Place, Dan Plakosh, *"System of Systems Interoperability (SOSI"): Final Report*, April 2004.
http://www.sei.cmu.edu/pub/documents/04.reports/pdf/04tr004.pdf#search=%22System%20of%20Systems%20Interoperability%20Final%20Report%22

O'May, Janet F. , Charles E. Hansen, Eric G. Heilman, Richard C. Kaste, Andrew M. Neiderer, "Battlespace Terrain Ownership: A New Situation Awareness Tool," *published in the proceedings of the 10th International Command and Control Research and Technology Symposium*, 13–16 June 2005.

O'Brien, Linsey , Scott Renner, Arnie Rosenthal, James Scarano, "Command Authority & Information Flows in Net-Centric Operations," *2006 CCRTS, The State of the Art and the State of the Practice*, The MITRE Corporation.

MOSNEWS news , *"Indonesia to Buy 12 Russian Submarines,"* January 2006
http://mosnews.com/news/2006/01/23/indonsub.shtml

Office of the Chief of Naval Operations**,** *"OPNAV Instruction 1000.16J, Manual of Navy Total Force Manpower Policies and Procedures,"* 17 June 2002

People's Daily news, *"Indonesian Navy to Buy Four Submarines from S. Korea,"* September 2003.
http://english.people.com.cn/200309/25/eng20030925_124937.shtml

Perry, Walter L., David Signori, John Boon, *Exploring Information Superiority: A Methodology for Measuring the Quality of Information and Its Impact on Shared Awareness*, Rand Corporation, May 2004.

Raney, Christopher John, "Integrating Multilevel Command and Control into a Service Oriented Architecture to Provide Cross Domain Capability," presented at *CCRTS 2006, The State of the Art and the State of the Practice,* SPAWAR Systems Center San Diego.

Spetka, Scott , George Ramseyer, Scot Tucker, Richard Linderman, Dennis Fitzgerald and Yan Lok-Kwong**,** *Net-Centric Pub/Sub Information Management Design for Command and Control*, Air Force Research Laboratory**,** 2006.

Steward, Mike, "FORCEnet: Networking the Naval Combat Force," *Defense Standardization Journal*, October/December 2004.

TTCP AG-6, *Operation Philippine Comfort Scenario* Coalition FORCEnet Study, V0.g, 2006.

TTCP AG-6, "*System Function Mapping to Levels of FORCEnet"* spreadsheet, July 2006.

TTCP Technical Report by Subcommittee on Non-Atomic Military Research and Development. *"Interpretation of TTCP MAR AG-1 Network Centric Warfare Study Tools and results in Terms of the FORCEnet Construct,"* December 2005.

Wickipedia , *"List of German Navy Ship Classes,"* July 2006.
http://en.wikipedia.org/wiki/List_of_ship_classes_of_the_Bundesmarine_and_Deutsche_Marine

World Navies Today news, "*World Navies Today: Indonesia,"* March 2002.
http://www.hazegray.org/worldnav/asiapac/indones.htm

THIS PAGE INTENTIONALLY LEFT BLANK

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California